Büllingen, Franz; Hillebrand, Annette

Working Paper

Sicherstellung der Überwachbarkeit der Telekommunikation: Ein Vergleich der Regelungen in den G7-Staaten

WIK Diskussionsbeitrag, No. 245

Provided in Cooperation with:
WIK Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste GmbH, Bad Honnef

Suggested Citation: Büllingen, Franz; Hillebrand, Annette (2003) : Sicherstellung der Überwachbarkeit der Telekommunikation: Ein Vergleich der Regelungen in den G7-Staaten, WIK Diskussionsbeitrag, No. 245, WIK Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste, Bad Honnef

This Version is available at:
https://hdl.handle.net/10419/226859

Sicherstellung der Überwachbarkeit der Telekommunikation

Ein Vergleich der Regelungen in den G7-Staaten

Franz Büllingen

Annette Hillebrand

Nr. 245

Juli 2003

Die vorliegende Untersuchung wurde im Auftrag des Bundesministeriums für Wirtschaft und Arbeit (BMWA) durchgeführt

wik Wissenschaftliches Institut für Kommunikationsdienste

WIK Wissenschaftliches Institut für
Infrastruktur und Kommunikationsdienste GmbH
Rhöndorfer Str. 68, 53604 Bad Honnef
Postfach 20 00, 53588 Bad Honnef
Tel 02224-9225-0
Fax 02224-9225-63
Internet: http://www.wik.org
eMail info@wik.org
Impressum

In den vom WIK herausgegebenen Diskussionsbeiträgen erscheinen in loser Folge Aufsätze und Vorträge von Mitarbeitern des Instituts sowie ausgewählte Zwischen- und Abschlussberichte von durchgeführten Forschungsprojekten. Mit der Herausgabe dieser Reihe bezweckt das WIK, über seine Tätigkeit zu informieren, Diskussionsanstöße zu geben, aber auch Anregungen von außen zu empfangen. Kritik und Kommentare sind deshalb jederzeit willkommen. Die in den verschiedenen Beiträgen zum Ausdruck kommenden Ansichten geben ausschließlich die Meinung der jeweiligen Autoren wieder.

ISSN 1865-8997

Inhaltsverzeichnis

Zusammenfassung

In einem demokratischen Rechtsstaat ist das Fernmeldegeheimnis unverletzlich. Überwachungsmaßnahmen der Telekommunikation (TK) unterliegen daher strengen rechtlichen Voraussetzungen. Eine Überwachung kann nur unter bestimmten Umständen angeordnet werden und die dabei erhobenen Daten unterliegen einer Zweckbindung.

Der dabei zu beachtende rechtliche Rahmen hat sich in den letzten Jahren auf Grund verschiedener Anforderungen verändert. Mit der Liberalisierung der Telekommunikationsmärkte wurde es für die nationalen Gesetzgeber notwendig, neue Regelungen zu formulieren, die alle TK-Anbieter und Betreiber von TK-Anlagen erfüllen müssen. Parallel dazu stellen neue TK-Dienste wie etwa E-Mail oder IP-Telefonie neue Herausforderungen an die Sicherstellung der Überwachbarkeit.

Die dazu erforderlichen gesetzlichen Änderungen wurden von kontroversen Diskussionen begleitet. Vor allem Verpflichtungen der TK-Anbieter und –Anlagenbetreiber zum Vorhalten technischer Einrichtungen und organisatorischer Vorkehrungen werden unter Kostengesichtspunkten von den Unternehmen kritisiert.

Die vorliegende Studie gibt vor diesem Hintergrund einen vergleichenden Überblick über die in Frankreich, Italien, Vereinigtes Königreich, USA, Kanada und Japan bestehenden rechtlichen Rahmenbedingungen. Im Mittelpunkt stehen die rechtlichen Grundlagen der Überwachung, die Verpflichtungen für die TK-Anbieter und Betreiber, die Voraussetzungen für sowie die Durchführung der Überwachung, die Kontroll- und Sanktionsmaßnahmen sowie die Aspekte der Kostenübernahme und Aufwandsentschädigungen.

Heute besitzen alle G7-Staaten Regelungen zur TK-Überwachung, jedoch unterschiedlich detailliert. Zu unterscheiden ist zwischen Ländern, die erst vor kurzem ein TK-Überwachungsgesetz verabschiedet haben (Japan) bzw. derzeit eine Aktualisierung hinsichtlich der Erweiterung der Verpflichtungen auf neue Technologien diskutieren (Kanada), und Ländern wie den USA und Deutschland, die nicht nur entsprechende Gesetze verabschiedet, sondern auch ausführliche Vorgaben zur Vorhaltung von Überwachungstechnik und organisatorische Maßgaben definiert haben. Das Vereinigte Königreich verabschiedete vor kurzem ähnliche Regelungen, ihre Implementierung hat jedoch gerade erst begonnen. In Frankreich und Italien sind die Vorgaben weniger detailliert und unterliegen teilweise der Geheimhaltung.

Obwohl in allen Ländern gesetzliche Regelungen existieren, verläuft die Umsetzung der TK-Überwachung in Bezug auf die Internet-Kommunikation überall mehr oder weniger problematisch, auch in Hinblick auf die jeweiligen kulturellen Besonderheiten. Diese spiegeln sich u.a. in dem Umgang mit Kontrollmaßnahmen und Datenmaterial zur TKÜ wieder. Während die USA, Deutschland, das Vereinigte Königreich und Kanada eine Vielzahl von Informationen für die Öffentlichkeit zur Verfügung stellen, auch z.B. über das WWW, ist Italien in diesem Punkt zurückhaltend. Auch in Frankreich und Japan sind Informationen weniger leicht öffentlich zugänglich.

Summary

Most countries enable their law enforcement and national security agencies to intercept telecommunication services under effectively controlled conditions. However lawful interception is only permitted due to defined circumstances. Gathered and stored data have to apply strictly to aimed purposes.

The framework of applicable law has substantially changed within the last few years. Due to the liberalisation of telecommunications markets, the market entry of new actors like internet service providers and the wide spread of digitized services, e.g. e-mail or IP-telephony the existing legal framework obviously had to be adapted to the new challenges in order to grant authorised law enforcement.

The change of the legal framework has been accompanied by intense and controversial debates on how actors should be obliged to establish procedures for responding to appropriate authorised requests. Criticisms of enterprises especially aime(d) at obligations to provide and implement the appropriate technical and organisational requirements, which are regarded as highly cost intensive.

Keeping this background in mind our study provides an overview on the existing framework in France, Italy, the United Kingdom, the USA, Canada and Japan in order to compare legal and practical measures. It focuses on the legal premises, the obligations of telecommunications service providers, the prerequisites and practices of lawful interception, the means of controlling and sanction as well as all aspects of the reimbursement of costs.

From today's perspective almost all G7-states have agreed on a generic set of requirements for legal interception differentiating only in details. Countries like Japan and Canada just have decided to implement rules on lawful interception respectively started to update their measures due to the modernisation processes in telecommunications technologies. Others like the US and Germany have finished their implementation processes regarding concrete technical and organisational measures, meanwhile the United Kingdom recently put a new legal framework into place, but the implementation of definite procedures is still at the beginning. In France and Italy regulation on lawful interception is less detailed than in the other countries.

Although the above mentioned states have set up a legal framework, the process of implementation and adoption of practices related to the internet face a lot of obstacles, e.g. the cultural background, influencing the national style of controlling measures and the handling of stored data. Furthermore the availability of information on lawful interception procedures differentiate between the countries. Whilst the US, Germany, the United Kingdom and Canada provide a more or less open access to relevant information, France and especially Italy are quite restrictive in permitting access to all information dealing with legal interception capabilities, procedures and results.

1 Einleitung

In einem demokratischen Rechtsstaat ist das Fernmeldegeheimnis unverletzlich. Überwachungsmaßnahmen der Telekommunikation (TK) unterliegen daher strengen rechtlichen Voraussetzungen. Nach diesem Prinzip ist auch die Sicherstellung der Überwachbarkeit der Telekommunikation in den G7-Staaten geregelt. Eine Überwachung kann nur unter bestimmten Umständen angeordnet werden und die dabei erhobenen Daten unterliegen einer Zweckbindung. In der Regel handelt es sich um Überwachungsmaßnahmen, die bei Verdacht bestimmter schwerer Straftaten und auf Grund schriftlicher richterlicher Anordnung eingeleitet werden. Die Überwachung erstreckt sich dabei nur auf benannte Verdachtspersonen bzw. auf genau definierte Kennungen, über die die Telekommunikation stattfindet.

Darüber hinaus existieren neben den Maßnahmen zur individuellen Kontrolle auch Möglichkeiten der strategischen Überwachung von Telekommunikation. Um präventiv gegen kriminelle Handlungen vorgehen zu können, wird im Rahmen derartiger Abhörmaßnahmen ein bestimmter Prozentsatz der Telekommunikation mit bestimmten ausländischen Gefahrengebieten überwacht, wobei kein Personenbezug gegeben ist. Auch diese Option ist in vielen Ländern gesetzlich vorgesehen.

Seit Einführung der gesetzlich geregelten Überwachbarkeit der Telekommunikation im Oktober 1968 sind in Deutschland die Überwachungszahlen ständig gestiegen. Dies gilt ebenso für andere Länder. Den Großteil der Maßnahmen machen dabei die individuellen Kontrollen aus. Dies weist auf veränderte Anforderungen der Strafverfolgungsbehörden hin, die angesichts der zunehmenden Nutzung neuer Telekommunikationsdienste stärker auf die Erkenntnisse der TK-Überwachung zur Verbrechensbekämpfung angewiesen sind.

Gleichzeitig mit der Liberalisierung der Telekommunikationsmärkte und dem damit verbundenen Auftreten verschiedener Wettbewerber statt eines Staatsmonopolisten auf dem Markt wurde es für die nationalen Gesetzgeber notwendig, neue Regelungen zu formulieren, die künftig alle TK-Anbieter und Betreiber von TK-Anlagen erfüllen müssen. In Deutschland wurden dazu beispielsweise bereits im Jahr 1989 entsprechende Anpassungen der gesetzlichen Regelungen im Rahmen der Gesetzgebung zu der ab 01.01.1990 wirksam gewordenen Privatisierung im Bereich der Telekommunikation vorgesehen. Darüber hinaus wurden nach Gesprächen mit den damaligen privaten Betreibern am 01.10.1993 „Rahmenbedingungen für die technische Gestaltung von Telekommunikationssystemen zur Ermöglichung der Durchführung von Überwachungsmaßnahmen nach G10 / §§ 100a, 100b StPO / AWG“ herausgegeben, die im Mai 1995 auf Grundlage des § 10b des Gesetzes über Fernmeldeanlagen durch eine entsprechende Rechtsverordnung ersetzt wurden (Fernmeldeverkehr-Überwachungs-Verordnung), die im Januar 2002 auf der Grundlage des § 88 des Telekommunikationsgesetzes durch die Telekommunikations-Überwachungsverordnung (TKÜV) abgelöst wurde.

Ferner hat sich der Kreis derer, die verpflichtet sind, den Strafverfolgungsbehörden die gesetzliche Überwachung von Telekommunikation zu ermöglichen, mit der Verbreitung und Nutzung neuer TK-Dienste erweitert. Die Überwachungsanforderungen gelten nämlich nicht nur für den Bereich der Sprachtelefonie, sondern auch für alle anderen Arten der Telekommunikation, wie früher Fernschreibverkehr oder heutzutage neue Angebote wie Datenkommunikation, E-Mail oder IP-Telefonie. Es ist abzusehen, dass dies künftig in der Mehrzahl der Staaten der Fall sein wird, auch wenn in manchen Ländern wie etwa in Kanada die Übertragbarkeit der bisherigen rechtlichen Grundlage auf die neuen Kommunikationstechnologien derzeit noch umstritten ist und sich deshalb die Umsetzung des geplanten Gesetzesvorhabens verzögert.

Darüber hinaus sind nach den Ereignissen in den USA vom 11. September 2001 in allen führenden Wirtschaftsnationen Überlegungen angestellt worden, wie die Terrorismusbekämpfung auf nationaler und auch auf internationaler Ebene verbessert werden kann. Dabei spielt die gesetzlich geregelte Überwachbarkeit der Telekommunikation eine bedeutende Rolle. Die Anti-Terrorgesetze, die in vielen Staaten erlassen wurden, stellen zum Teil weitergehende Anforderungen als bisher an die TK-Anbieter und Betreiber von TK-Anlagen.

Überwachungsmaßnahmen sind jedoch nicht nur im Zusammenhang mit den jüngsten Entwicklungen erforderlich geworden, sondern werden in der Regel schon seit einigen Jahrzehnten durchgeführt, auch wenn nicht immer eine eigene Gesetzesgrundlage dafür vorlag. So ist beispielsweise im Vereinigten Königreich im Jahr 1985 ein Gesetz zu Lawful Interception (LI) verabschiedet worden. In Japan besteht erst seit Sommer 2000 eine entsprechende gesetzliche Regelung. In Deutschland wurde die gesetzliche Grundlage im Jahr 1968 geschaffen, und zwar im Zuge der strafprozessualen Fernmeldeüberwachung als Teil der Notstandsgesetzgebung. Der Regelungsrahmen wird heute durch die Strafprozessordnung, durch das Gesetz zu Art. 10 des Grundgesetzes sowie das Außenwirtschaftsgesetz vorgegeben.

Aus der Tatsache, dass in allen europäischen Ländern wie auch in den USA und Kanada Überwachungsmaßnahmen seit Jahrzehnten als Mittel der Strafverfolgung eingesetzt werden, darf jedoch nicht geschlossen werden, dass in diesen Staaten die Einführung bzw. Durchführung dieser Maßnahmen ohne Diskussionen verläuft. Datenschutzbehörden und zahlreiche Privacy-NGOs begleiten die Entwicklung in diesem Bereich regelmäßig mit kritischen Stellungnahmen.

Um dieser Kritik zu begegnen, haben beinahe alle G7-Staaten, wie etwa auch Frankreich oder Deutschland, die Überwachung unter Richtervorbehalt gestellt oder zur demokratischen Kontrolle der Überwachungsaktivitäten Kommissionen eingerichtet bzw. Behörden mit dem Erstellen von Statistiken in diesem Zusammenhang beauftragt.

Bei den TK-Unternehmen stoßen die Regelungen zur gesetzlichen Überwachung häufig auf Kritik, weil diese Maßnahmen kosten- und zeitaufwändig sind. Nicht nur in Deutsch-

land müssen die verpflichteten TK-Unternehmen die entstehenden Kosten für netzseitige Vorkehrungen beinahe vollständig selbst tragen. Dies ist auch in anderen Staaten wie etwa im Vereinigten Königreich oder in Kanada ein Hauptstreitpunkt, der im Zuge der Anforderungen an die Überwachbarkeit der Internet-Kommunikation an Intensität gewinnt. Im Zuge der Verabschiedung der TKÜV hatten die deutschen Internet Service Provider (ISP) die technischen und organisatorischen Überwachungsanforderungen sogar als Markthemmnis bewertet und gefordert, von den Anforderungen der Verordnung weitgehend ausgenommen zu werden. In den meisten Ländern wird zurzeit darüber diskutiert, wie ein Kompromissvorschlag aussehen könnte.

Anforderungen an die Unternehmen hinsichtlich der Ermöglichung von Überwachungsmaßnahmen ergeben sich aber nicht nur aus der nationalen Gesetzgebung. Durch die Zunahme von Kriminalitätsformen im Bereich des internationalen Terrorismus entstehen heute neue Erfordernisse hinsichtlich des Datenaustauschs unter verschiedenen nationalen Behörden. Die europäischen Staaten sowie führende Wirtschaftsnationen wie die USA, Japan und Kanada bemühen sich um eine stärkere Zusammenarbeit bei der Verbrechensbekämpfung.

Auf europäischer Ebene ist man bestrebt, eine Harmonisierung der Regelungen herbeizuführen. Dazu besteht beispielsweise die Entschließung des Rates vom 17. Januar 1995 über die rechtmäßige Überwachung des Fernmeldeverkehrs. Darin wird angeregt, im Rahmen der allein maßgebenden nationalen Gesetzgebung die Anforderungen der Strafverfolgungsbehörden hinsichtlich der Überwachung der Telekommunikation umzusetzen. Die Europäischen Strafverfolgungsbehörden fordern, dass ein Zugriff auf alle Arten der Telekommunikation gewährleistet werden kann. Zur Erläuterung der Entschließung hinsichtlich moderner Telekommunikationsdienste wird seit geraumer Zeit ein Papier diskutiert, dass u. a. unter den Bezeichnungen ENFOPOL 98 und ENFOPOL 55 bekannt geworden ist. Die Novellierung der europäischen Datenschutzrichtlinie trägt ebenfalls zur Vereinheitlichung der Bestimmungen bezüglich der Überwachbarkeit bei. Hier steht derzeit die Anforderung der Datenspeicherung (Data Retention) im Mittelpunkt der kontroversen Diskussion.

Auch die Ende 2001 verabschiedete Cybercrime-Convention des Europarates hat eine verbesserte Zusammenarbeit hinsichtlich der Möglichkeit der Verfolgung von Straftaten im Bereich der Internet-Kommunikation und eines verbesserten grenzüberschreitenden Datenaustausches zum Ziel. Die G7-Staaten verständigten sich ebenfalls im Jahr 2001 auf eine stärkere Zusammenarbeit. Das vereinbarte Ziel „Fighting Terrorism“ wurde von allen Mitgliedsstaaten durch das Erlassen von neuen bzw. die Erweiterung von bestehenden Regelungen umgesetzt.

Ziel der vorliegenden Untersuchung ist es, einen vergleichenden Überblick über die in den G7-Staaten – Frankreich, Italien, Vereinigtes Königreich, USA, Kanada und Japan – mit den in Deutschland bestehenden rechtlichen Rahmenbedingungen in Bezug auf die Sicherstellung der Überwachbarkeit der Telekommunikation zu erstellen.

Dabei ist insbesondere zu betrachten, welche veränderten Anforderungen an die Unternehmen sich zum Einen aus der Liberalisierung und Privatisierung der TK-Märkte sowie zum Anderen aus technologischen Innovationen (z.B. IP-Telefonie, E-Mail-Kommunikation) ergeben.

Des Weiteren soll herausgearbeitet werden, welche Gemeinsamkeiten bzw. Unterschiede in den Regelungen daraus erwachsen, dass die zu untersuchenden Staaten Mitglieder bzw. Nicht-Mitglieder der Europäischen Union sind. Dabei ist zu beachten, aus welchen spezifischen nationalen Vorschriften sich ggf. Konflikte in Hinblick auf die Vorgaben der EU in Bezug auf einen freien Marktzutritt ergeben könnten.

Die Studie wurde im Auftrag des Bundesministeriums für Wirtschaft und Arbei (BMWA) durchgeführt. Sie basiert neben Dokumentenanalysen und Literaturauswertungen auf intensiven Recherchen bei verschiedenen ausländischen Institutionen. Die Autoren sind diesen Experten und Organisationen für ihre Hinweise und Informationen zu Dank verpflichtet.[1]

1 Eine Liste der Experten und Organisationen liegt dem Auftraggeber vor. Sie ist vertraulich.

2 Zentrale Fragestellungen

Folgende Fragestellungen erscheinen bezüglich der Sicherstellung der Überwachbarkeit der Telekommunikation relevant und sollen für die einzelnen Länder betrachtet werden:

- **Rechtliche Grundlagen der Überwachung:** Welche Bereiche der TK-Gesetzgebung bilden die rechtliche Grundlage für die Überwachung? Welche einschlägigen Rechtsvorschriften sind bei der Durchführung von Überwachungsmaßnahmen und für evtl. im Vorfeld zu treffende Vorkehrungen zu beachten? Für welche Dienste gelten die Regelungen? Welche Gesetze betreffen die individuelle Überwachung, welche die strategische Überwachung?

- **Verpflichtungen für die TK-Anbieter und Betreiber von TK-Anlagen:** Seit wann müssen die Unternehmen bei der Überwachung unterstützend tätig werden? Wer – z.B. alle Netzbetreiber, alle ISP, nur lizenzpflichtige Anbieter - muss technische und organisatorische Vorkehrungen treffen? Sind diese ständig oder nur fallweise vorzuhalten? Welche Ausnahmen gibt es, z.B. hinsichtlich der gewerblichen bzw. nichtgewerblichen Absichten eines Anbieters/Betreibers oder hinsichtlich der Größe (z.B. ausgedrückt durch die angeschlossenen Teilnehmer)? Wie und wo sind die technischen und organisatorischen Anforderungen spezifiziert? Wer kontrolliert, ob diese erfüllt werden, z.B. gibt es Genehmigungsverfahren für technische Überwachungseinrichtungen? Wo sind ggf. Kollisionen mit EU-Regelungen festzustellen (nur hinsichtlich EU-Mitgliedstaaten)?

- **Voraussetzung für die Überwachung:** In welchen Fällen muss das Überwachen oder Aufzeichnen der Telekommunikation ermöglicht werden? In welchen Fällen ist z.B. eine richterliche Anordnung erforderlich, in welchen nicht? Muss das Unternehmen die Rechtmäßigkeit der Anordnung überprüfen? Sind Echtzeit-Überwachungen oder ist die Speicherung von Telekommunikationsdaten vorgesehen? Wer muss wie lange Daten speichern?

- **Durchführung der Überwachung:** Wer und was wird überwacht? Wie wird die zu überwachende Telekommunikation an die Behörden übermittelt? Welche Angaben sind erforderlich, um einen Überwachungsvorgang einzuleiten? Welche Kennungen müssen die Strafverfolgungsbehörden den Unternehmen nennen? Welche Daten werden überwacht? Nur Individualkommunikation oder auch weiteres? Dürfen nur Daten der Telekommunikation oder auch Dienste überwacht werden? Werden sowohl die Begleitumstände der Kommunikation als auch die Inhalte an die Strafverfolgungsbehörden weitergeleitet? Welche Unterschiede existieren zwischen individueller und strategischer Überwachung? Müssen für verschiedene Überwachungsanforderungen unterschiedliche technische Einrichtungen vorgehalten werden?

- **Kontroll- und Sanktionsmaßnahmen:** Welche Berichtspflichten sind vorgesehen? Werden Statistiken über die durchgeführten Überwachungsmaßnahmen geführt? Von wem? Welche Kontrollinstanzen existieren? Mit welchen Sanktionen muss ein Unternehmen rechnen, dass gegen die rechtlichen Vorschriften zur Überwachung verstößt?

- **Kostenübernahme und Aufwandsentschädigungen:** Wer trägt die Kosten für die netzseitigen technischen und organisatorischen Vorkehrungen? Wer trägt die Kosten für die Übermittlung an die berechtigten Stellen? Gibt es eine Aufwandsentschädigung für tatsächlich durchgeführte Maßnahmen? Wie wird der Aufwand für die Überwachungsmaßnahmen von den dazu verpflichteten Unternehmen bewertet? Stellen die Anforderungen aus ihrer Sicht ein Markthemmnis dar?

3 Rahmenbedingungen für Lawful Interception in der EU

3.1 Rechtliche Grundlagen in der EU – Stand und aktuelle Diskussion

Auf europäischer Ebene sind Bestimmungen zur Sicherstellung der Überwachbarkeit der Telekommunikation und der Datenspeicherung u.a. im Rahmen des Datenschutzes sowie der Europäischen Menschenrechtskonvention angesprochen.[2] Wichtige Weichenstellungen sind außerdem implizit in den Planungen zu einer Verbesserung der Sicherheit im Internet enthalten. Aktuell sind darüber hinaus die Cybercrime Konvention des Europarates, die Planungen im Rahmen von Europol sowie die Vereinbarungen der G7/G8-Staaten von Bedeutung für die derzeitige Diskussion.

3.1.1 Allgemeine Datenschutzbestimmungen (95/46/EG)

Allgemeine Datenschutzbestimmungen sind in der Richtlinie 95/46/EG[3] niedergelegt. Mit der Novellierung des Bundesdatenschutzgesetzes im Mai 2001 wurden die Bestimmungen in Deutschland umgesetzt. Die Länder Brandenburg, Baden-Württemberg, Bayern, Hessen, Nordrhein-Westfalen und Schleswig-Holstein haben diese auch bereits in ihre Landesgesetze aufgenommen.

Wesentliche Punkte der Richtlinie umfassen die Maßgabe, dass alle Mitgliedsländer die Rechte und Freiheiten natürlicher Personen in Bezug auf die elektronische Datenverarbeitung respektieren müssen. Ziel ist, einen ungehinderten Datenverkehr in der Europäischen Union sicherzustellen. Die dazu in den Ländern getroffenen Maßnahmen müssen im Einklang mit der Europäischen Menschenrechtskonvention stehen.

In Art. 13 der Richtlinie ist festgelegt, unter welchen Voraussetzungen Rechte in Bezug auf den Datenschutz eingeschränkt und Pflichten zur Unterstützung der Strafverfolgungsbehörden auferlegt werden können. Eine Beschränkung kann u.a. aus diesen Gründen erfolgen: Sicherheit eines Staates, Landesverteidigung, öffentliche Sicherheit, Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten, wichtige wirtschaftliche oder finanzielle Interessen, die Wahrnehmung von Kontroll-, Überwachungs- und Ordnungsfunktionen sowie der Schutz von Personen und der Rechte und Freiheiten anderer Personen.

---

2 Das Themenfeld Datenschutz berührt nicht das Themenfeld Überwachung der Telekommunikation im engeren Sinne. Da jedoch Anforderungen bezüglich der Datenspeicherung zurzeit im Mittelpunkt der Diskussion um die Verpflichtungen der ISP stehen, werden die Regelungen in dieser Studie an geeigneter Stelle skizziert.

3 Kommission der Europäischen Gemeinschaften (1995).

3.1.2 TK-Datenschutz-Richtlinie der EU (2002/58/EG)

Die Revision der EU-TK-Datenschutz-Richtlinie 97/66/EG[4] im Mai 2002 zur neuen TK-Datenschutz-Richtlinie 2002/58/EG[5] stand lange Zeit im Mittelpunkt einer kontroversen Diskussion. Davon waren nicht die Regelungen bezüglich Lawful Interception betroffen. In der neuen wie auch in der zuvor geltenden TK-Datenschutzrichtlinie werden ausdrücklich nicht die Möglichkeiten der jeweiligen Staaten eingeschränkt, Maßnahmen im Bereich des „Lawful Interception" zu ergreifen und dazu eigene Gesetze zu erlassen. Die Harmonisierungsbestrebungen beschränken sich auf Regelungen zu Speicherung, Weiterverarbeitung und Verwendung personenbezogener Daten in Bezug auf Abrechnungen, insbesondere Einzelverbindungsnachweise, persönliche Kundendaten und beim Telekommunikationsvorgang generierte Verbindungsdaten[6], und betreffen nicht Regelungen zur TK-Überwachung.

Die neue TK-Datenschutz-Richtlinie unterscheidet sich nur graduell von der vorhergehenden. Sie enthält in Art. 15 Bestimmungen, nach denen der TK-Datenschutz eingeschränkt werden kann. Dabei wird Bezug genommen auf die allgemeine EU-Datenschutz-Richtlinie (Art. 13, s.o.). Wie auch die vorhergehende Richtlinie festlegte, können die Mitgliedstaaten Rechtsvorschriften erlassen, soweit es für die „nationale Sicherheit (d.h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig" ist. Letztere Formulierung stellt eine Ausweitung der bisher gültigen Bestimmung dar, die sich auf den „unzulässigen Gebrauch von Telekommunikationssystemen" beschränkte. Somit sind in die neue Richtlinie alle elektronischen Kommunikationsmittel, wie z.B. auch internetbasierte Dienste, ausdrücklich eingeschlossen.

Neu ist auch die daran anschließende Formulierung, welche den Ländern die Möglichkeit eröffnet, Daten (Verkehrsdaten und Standortdaten) durch die Diensteanbieter speichern zu lassen: „Zu diesem Zweck können die Mitgliedstaaten unter anderem durch Rechtsvorschriften vorsehen, dass Daten aus den in diesem Absatz aufgeführten Gründen während einer begrenzten Zeit aufbewahrt werden."

Im Zusammenhang mit der Richtlinie wurden Mindestspeicherfristen von bis zu 12 Monaten diskutiert, jedoch konnten sich die Mitglieder auf keine Fristen einigen. Auch die Mitglieder des EU-Rates betonten in den der Richtlinie vorangehenden Erwägungsgründen die nationalen Zuständigkeiten und verzichteten auf die Nennung von Spei-

---

4 Kommission der Europäischen Gemeinschaften (1997).
5 Kommission der Europäischen Gemeinschaften (2002).
6 Im Zuge der neuen technischen Möglichkeiten unterscheidet man heute Verkehrsdaten (engl. traffic data, d.h. Daten, die zur Abwicklung der Telekommunikation notwendig sind) sowie Standortdaten (Daten, die z.B. im Mobilfunk den geographischen Standpunkt des TK-Nutzers enthalten.). Im Text wird für Verkehrsdaten auch der Ausdruck Kommunikationsdaten verwendet.

cherfristen. Sie wiesen jedoch darauf hin, dass Regelungen dieser Art im Einklang mit der EMRK stehen müssen. In Deutschland ist „Vorratsdatenspeicherung“ bisher ausdrücklich untersagt.[7] Andere Länder wie das Vereinigte Königreich lassen Datenspeicherung über die für Rechnungszwecke notwendigen Fristen hinaus zu.

Ein vom Bundesrat eingebrachter Gesetzentwurf[8] enthält Vorschläge, wonach der § 89 des TKG dahingehend geändert werden soll, dass neben Datenschutzvorschriften auch Regelungen zur „Vorratsspeicherung“ aufgenommen werden. Statt der jetzt geltenden Regelung zu Höchstfristen für die Speicherung von Verbindungsdaten sollen „Mindestfristen“ vorgesehen werden. Es ist beabsichtigt, eine sinngemäße Regelung in das Teledienstedatenschutzgesetz (TDDSG) einzufügen. Hintergrund der Pläne zur Festlegung von Speicherfristen ist, dass heute die TK-Unternehmen Daten nur zum Zweck der Rechnungstellung und Diensteerbringung speichern dürfen. Die Höchstspeicherfrist, während der die Daten aufbewahrt werden können (nicht müssen), beträgt 6 Monate. Faktisch löschen viele Netzbetreiber die Daten bereits vorher, um die mit der Speicherung verbundenen Kosten zu senken.

Die Bundesregierung hat den Gesetzentwurf des Bundesrates abgelehnt mit der Begründung, zwischen Datenschutz und den Erfordernissen der Strafverfolgung sei ein Interessenausgleich herbeizuführen. Eine Entscheidung über den Gesetzentwurf im Bundestag steht noch aus.

Unternehmen befürchten eine Zunahme der Verpflichtungen und protestieren daher gegen die Option der „Vorratsdatenspeicherung“ vor allem aus Kostengründen.

Welche weiteren Änderungsvorschläge sich in Bezug auf die deutsche Gesetzgebung, u.a. bei der Novellierung des TKG, durch die von der EU-Richtlinie zugelassene Erlaubnis der Datenspeicherung für eine begrenzte Zeit ergeben können, ist heute noch nicht absehbar. Die Richtlinie muss von den Mitgliedstaaten bis zum 31. Oktober 2003 in nationale Rechtsvorschriften umgesetzt werden.[9]

3.1.3 Mitteilung der EU-Kommission: Schaffung einer sichereren Informationsgesellschaft im Rahmen der Initiative eEurope 2002

Die Mitteilung der EU-Kommission „Schaffung einer sichereren Informationsgesellschaft“[10] setzt sich ebenfalls mit der Datenschutzproblematik der Datenspeicherung auseinander (insbes. Kap. 5.1 und 5.2), jedoch nicht mit der TK-Überwachung. Das

---

7 Vgl. die Leitsätze zum Urteil des Ersten Senats des Bundesverfassungsgerichts vom 15. Dezember 1983 zum Volkszählungsgesetz 1983 (1 BvR 209/83 u.a.).

8 Vgl. Deutscher Bundestag (2002).

9 Datenschutzexperten weisen darauf hin, dass das BVerfG die zweckoffene Datenspeicherung nicht anonymisierter personenbezogener Daten für verfassungswidrig erklärt hat (BVerfGE 65, 1, 46), vgl. Bäumler, H. u.a. (2002).

10 Kommission der Europäischen Gemeinschaften (2001).

Papier diente als Diskussionsgrundlage für eine Entscheidungsfindung. Im Rahmen der Veröffentlichung der Mitteilung wurde eine Anhörung durchgeführt. In der Mitteilung wird betont, dass laut EU-Datenschutzrichtlinien die Pflichten zur Datenlöschung an die nationalen Sicherheitsanforderungen angepasst werden dürfen.

3.2 Weitere relevante internationale Vereinbarungen im europäischen Kontext

Über die Bestimmungen im Rahmen von EU-Richtlinien hinaus existieren Vereinbarungen auf europäischer Ebene, die Einfluss auf die nationalen Bestimmungen zu LI haben, auch wenn sie nicht direkt die gesetzlichen TK-Überwachungsregelungen betreffen.

3.2.1 Europäische Menschenrechtskonvention (EMRK)

Nach der Europäischen Menschenrechtskonvention (EMRK) des Europarates ist jegliche Überwachung von EU-Bürgern oder Unternehmen als tiefgreifender Eingriff in die Privatsphäre nach Art. 8 zu werten. Nur zur Gewährleistung der nationalen Sicherheit, der öffentlichen Ruhe und Ordnung, des wirtschaftlichen Wohls eines Landes, der Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer sind Eingriffe in dieses Recht zulässig. Diese müssen gesetzlich legitimiert sein. Unzulässig sind Überwachungen, die nicht auf der Grundlage allgemein zugänglicher, gesetzlicher Regelungen erfolgen.[11]

3.2.2 Cybercrime Konvention des Europarates

Die Cybercrime Konvention des Europarats ist am 23. November 2001 von der Bundesrepublik sowie von weiteren Staaten unterzeichnet worden, sie ist allerdings bisher nur von wenigen Staaten ratifiziert worden und noch nicht in Kraft getreten. Alle G7-Staaten sind der Konvention beigetreten. In Art. 20 der Konvention ist festgehalten, nach welchen Regelungen Verbindungs- und Nutzungsdaten der elektronischen Kommunikation gespeichert werden sollen. Es sollen nur „specific communications“, d.h. nicht alle Kommunikationsvorgänge erfasst werden.

---

11 Vgl. die Konvention des Europarates zum Schutze der Menschenrechte und Grundfreiheiten in der Fassung des Protokolls Nr. 11, Art. 8 sowie die Ausführungen bei Bizer, J. (2002), S. 484.

3.2.3 EUROPOL

Die European Police Office EUROPOL hat sich ebenfalls mit dem Thema Lawful Interception und Data Retention auseinandergesetzt. In einem vor kurzem diskutierten Arbeitspapier wurden die Anforderungen der Strafverfolgungsbehörden an die TK-Anbieter und Betreiber von TK-Anlagen formuliert.[12] Die Liste enthält Angaben zu Internet-Kennungen wie Network Access, E-Mail, Web Servers, Usenet, Internet Relay Chat sowie Kennungen im Zusammenhang mit Festnetz- und Mobilfunkkommunikation.

3.2.4 Vereinbarung auf Ebene der G7/G8-Staaten

Die G7/G8-Staaten haben sich auf ihrer Versammlung in Genua 2001 auf einen umfassenden Katalog von Vorkehrungen bezüglich der Bekämpfung des Terrorismus geeinigt. Das Programm „Fighting Terrorism“ berührt indirekt auch die Sicherstellung der Überwachbarkeit der Telekommunikation, der Schwerpunkt liegt aber auf Maßnahmen in folgenden Bereichen:

- Ausschöpfen der Maßnahmen im Bereich Finanzen, um die Kapitalflüsse der Terroristen zu stoppen,
- Flugsicherheit,
- Waffenexportkontrolle,
- Kooperation der Strafverfolgungsbehörden und anderer Sicherheitsbehörden,
- die Ablehnung aller Mittel, die Terrorismus befördern können,
- die Identifizierung und die Beseitigung von terroristischen Bedrohungen.

Alle Mitgliedsländer haben ihre politischen Aktivitäten in diesen Bereichen verstärkt und eigene Anti-Terrorgesetze erlassen. Zum Teil beinhalten diese Regelungen auch Maßnahmen in Bezug auf TK-Überwachung und Data Retention.[13]

Im Bereich Data Retention und Lawful Interception sind von den G7/G8-Staaten folgende Stellungnahmen und Empfehlungen veröffentlicht worden:[14]

- Principles on Transborder Access to Stored Computer Data,

---

12 Vgl. EUROPOL (2001).
13 Vgl. zum Stand der Umsetzung des Ziels die Untersuchung von Kirton, J.; Kokotsis, E. (2002).
14 Siehe dazu u.a. die Hinweise unter http://www.g8j-i.ca/english/intro.html, anlässlich des G8 Justice and Interior Ministers’ Meeting in Mont-Tremblant, Canada, 2002.

- Recommendations for Tracing Networked Communications Across National Borders in Terrorist and Criminal Investigations,
- Issues to Be Considered in a Legal Framework for Data Preservation,
- Law Enforcement Record Preservation Checklist,
- Principles on the Availability of Data Essential to Protecting Public Safety.

Diese Dokumente sind nicht bindend, geben jedoch Hinweise darauf, wie Regelungen insbesondere auf dem Gebiet Data Retention in den Mitgliedsstaaten vereinheitlicht werden könnten.

4 Rahmenbedingungen für Lawful Interception in Frankreich

Frankreich besitzt Regelungen sowohl zu Lawful Interception als auch zu Data Retention. Die Sicherstellung der Überwachung der Telekommunikation beruht auf einem Gesetz aus dem Jahr 1991. Der Europäische Gerichtshof für Menschenrechte hatte ein Urteil gegen Frankreich wegen Verstoß gegen Art. 8 EMRK gefällt. Aufgrund dieser Entscheidung im Jahr 1990 wurde eine gesetzliche Grundlage für Lawful Interception geschaffen.[15]

Die Datenspeicherung ist seit 2001 rechtlich geregelt. Die Bestimmungen betreffen vorrangig Internet Service Provider.

Die Überwachung der Internet-Kommunikation ist auch in Frankreich eine zentrales Thema. Die Verpflichtungen der ISP gegenüber den berechtigten Stellen sind jedoch nicht öffentlich zugänglich. Die dazu in den Expertengesprächen gemachten Ausführungen lassen erkennen, dass permanente technische Ausstattungen auf Seiten der ISP sowie auch auf Seiten der berechtigten Stellen noch nicht überall vorhanden sind.

4.1 Rechtliche Grundlagen

4.1.1 Grundlagen in der TK-Gesetzgebung

Der französische Gesetzgeber hat in den einschlägigen Vorschriften festgelegt, dass sich die Sicherstellung der Überwachbarkeit auf die gesamte Telekommunikation im Sinne des französischen TKG bezieht.[16] Damit geht die Regelung über das Abhören der Sprachtelefonie hinaus und erstreckt sich auf alle modernen Formen der elektronischen Kommunikation.[17]

4.1.2 Einschlägige Rechtsvorschriften

Das für die TK-Überwachung einschlägige Gesetz ist das

- Loi n° 91-636 du 10 juilliet 1991 relative au secret des correspondances émises par la voie des télécommunications.

Das Gesetz fügt im Rahmen des ersten Gesetzestitels „Abhörungen auf Anordnung der Justizbehörden“ in die Strafprozessordnung (Code de procédure pénale (c.p.p.)) die

---

15 Vgl. EPIC/PI (Eds.) (2002), S. 178 sowie Lücking, E. (1992), S. 120f.
16 Vgl. Art. L. 32, 1° Code des postes et télécommunications.
17 Vgl. Lücking, E. (1992), S. 124.

Art. 100 bis 100-7 ein.[18] Der Titel II umfasst die Regelungen zu den sog. sicherheitsbedingten (präventiven) TK-Überwachungen.[19]

In der Verordnung

- Décret n° 93-119 du 28 janvier 1993, Décret relatif à la désignation des agents qualifiés pour la réalisation des opérations matérielles nécessaires à la mise en place des interceptions de correspondances émises par voie de télécommunications autorisées par la loi n° 91-646 du 10 juillet 1991

sind allgemeine organisatorische Sicherheitsvorkehrungen festgelegt, die sowohl die berechtigten Stellen als auch die Unternehmen betreffen.

Technische Richtlinien, die die Verpflichtungen der TK-Anbieter und –Anlagenbetreiber spezifizieren, existieren nicht.

Das TK-Überwachungsgesetz von 1991 löst die im Jahr 1960 erstmals getroffenen rechtlichen Regelungen in diesem Bereich ab. Entscheidende Änderung ist die stärkere Kontrolle der Durchführung der präventiven Überwachungsmaßnahmen durch eine neu gegründete Behörde, die CNCIS (Commission nationale de contrôle des interceptions de sécurité), eine nationale, unabhängige Kontrollbehörde (Art. 13, Loi n° 91-636 du 10 juilliet 1991).

Data Retention

Die Datenspeicherung ist geregelt im

- Loi sur la sécurité quotidienne (LSQ) („Gesetz über Sicherheit im Alltag“),[20]

das im Zuge der Aktivitäten zur Bekämpfung des Terrorismus nach den Ereignissen des 11. September im November 2001 erlassen wurde.

Das Gesetz regelt Ausnahmen von der Pflicht, Kommunikationsdaten unverzüglich zu löschen oder zu anonymisieren, wenn sie nicht mehr für die Erbringung der Dienstleistung benötigt werden. Nach dem neuen Gesetz wird es zur Pflicht, Daten für die Ermittlung, Beweisführung oder Anklage in Zusammenhang mit einer strafrechtlichen Handlung für die Dauer von einem Jahr zu speichern. Die Speicherung für Abrechnungszwecke ist nunmehr freiwillig.

Weiterführende Regelungen waren im geplanten Loi sur la société de l’information (LSI) formuliert, welches die Implementation der EU-Richtlinie zu Electronic Commerce zum

---

18 Diese dienen zur Konkretisierung des Art. 81 c.p.p., der eine generelle Ermächtigung zur Ergreifung von Maßnahmen enthält, die zur Aufrechterhaltung der öffentlichen Sicherheit und Ordnung sowie der Verhinderung und der Verfolgung von Verbrechen dienen (vgl. Lücking, E. (1992), S. 125).

19 Vgl. CNCIS (o.J.), S. 3.

20 Loi n°2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne.

Ziel hatte. Aufgrund des Regierungswechsels im Jahr 2002 wurde das Gesetz, das auf starke Proteste der Datenschutzorganisationen gestoßen ist, nicht wie geplant verabschiedet.

4.1.3 TK-Dienste, für die die Überwachbarkeit gewährleistet sein muss

Grundsätzlich ist für alle Dienste, die nach dem französischen TKG als Telekommunikation gelten, die Überwachbarkeit zu gewährleisten. Damit kann die Gesetzesgrundlage insofern als technikoffen bezeichnet werden, als sie keine Form der elektronischen Kommunikation ausschließt. Beispielhaft werden in der Gesetzesbegründung zum TK-Überwachungsgesetz Minitel, Telefax, Telex sowie Funktelefone genannt.[21]

4.1.4 Zweck der Überwachung

Der Zweck der Überwachung der Telekommunikation – gestützt auf die Strafprozessordnung – liegt sowohl in der individuellen Aufklärung von Straftaten und der Überführung der Täter als auch auf präventiver, also strategischer Ebene. Die Daten einer richterlichen angeordneten Überwachungsmaßnahme können von Anklage und Verteidigung im Rahmen von Gerichtsverfahren eingesehen werden und dienen als Beweismittel.

4.1.5 Unterschiede zwischen Überwachungsmaßnahmen der Strafverfolgungsbehörden und denen der Sicherheitsbehörden

Das TK-Überwachungsgesetz unterscheidet „écoutes judiciaires“ (richterliche TK-Überwachungen), also die von einem Richter angeordneten individuellen Überwachungen zum Zweck der Strafverfolgung (Art. 2 Loi n° 91-636 du 10 juilliet 1991) und die „écoutes administratives“ bzw. auch „interceptions de sécurité“ (administrative TK-Überwachungen) (Art. 3 bis 19, Loi n° 91-636 du 10 juilliet 1991). Letzteren liegen präventive und informative Ziele zugrunde und nicht das Ziel Beweismittel zu sammeln.[22]

Für die Anzahl der „interceptions de sécurité“ werden vom Premierminister Quoten für die berechtigten Ministerien festgelegt. Die Gesamtzahl der grundsätzlich genehmigungsfähigen TK-Überwachungen für ein Jahr darf zu keiner Zeit überschritten werden.

---

21 Vgl. Lücking, E. (1992), S. 124.

22 Vgl. Lücking, E. (1992), S. 125. „Interceptions de sécurité“ bezeichnen eine Form der strategischen Überwachung, die sich von der deutschen Definition von strategischer Überwachung insofern unterscheidet, als die Überwachung in Frankreich ebenfalls nicht anlass-, aber personenbezogen durchgeführt wird.

Die Zahl wurde zum 1. Januar 2003 von zuvor 1.540 Maßnahmen (seit 1997) auf insgesamt 1.670 Maßnahmen leicht erhöht. Die Anzahl der möglichen TK-Überwachungen pro Jahr verteilt sich auf folgende Weise:[23]

- 1.190 für das Innenministerium (keine Erhöhung). Zu dem Bereich des Innenministeriums gehört z.B. die Police, die Police judiciaire sowie der Inlandsgeheimdienst DST,
- 400 für das Verteidigungsministerium (zuvor: 330). Dazu gehört z.B. die Gendarmerie sowie der Auslandsgeheimdienst DGSE.
- 80 für das für den Zoll verantwortliche Finanzministerium (zuvor: 20).

Bezüglich der Anzahl von „écoutes judiciaires“ existieren keine Beschränkungen.

Es dürfen aber keinerlei Überschneidungen zwischen den richterlichen und den administrativen Überwachungen auftreten. Die von einem Untersuchungsrichter angeordnete Abhörung unterbricht automatisch eine eventuell bestehende „interception de sécurité“. Letztere darf nicht mehr durchgeführt werden, wenn eine gerichtlich angeordnete Abhörmaßnahmen bereits stattgefunden hat.[24]

Verboten ist auch die gleichzeitige Überwachung eines Anschlusses durch mehrere berechtigte Stellen. Es besteht ebenfalls nicht die Möglichkeit, die Daten einer anderen berechtigten Stelle für eigene Untersuchungszwecke anzufordern und auszuwerten.

Aus technischer Sicht bzw. im Hinblick auf das Vorhalten von technischen oder organisatorischen Einrichtungen bestehen für die Unternehmen keine Unterschiede zwischen gerichtlich und präventiv angeordneten TK-Überwachungen.

4.2 Verpflichtungen für die TK-Anbieter und Betreiber von TK-Anlagen

4.2.1 Kreis der Verpflichteten

Die französische Regulierungsbehörde ART (Autorité de régulation des télécommunications) hat mehrfach klargestellt, dass auf Basis der gesetzlichen Regelungen zum Kreis der Verpflichteten alle TK-Anbieter und –TK-Anlagenbetreiber gehören, also auch z.B. die ISP. Derselben Auffassung ist die Kontrollbehörde CNCIS, die die Einhaltung der

---

23 Vgl. CNCIS (o.J.), S. 5, handschriftlicher Zusatz. Es handelt sich um die Anzahl der angeordneten Maßnahmen. Diese beziehen sich jeweils auf Kennungen, so dass die Anzahl nicht notwendigerweise mit der Anzahl der überwachten Personen identisch ist.

24 Vgl. CNCIS (o.J.), S. 7. Die Festlegung von Quoten ist ein Überbleibsel aus der Zeit, als technische Restriktionen die Anzahl der Überwachungsmaßnahmen einschränkten. Die Regelung wurde auch nach der Digitalisierung der Kommunikation aus Kontrollgründen beibehalten.

Regeln für präventive TK-Überwachung kontrolliert. Die Verpflichtung zur Unterstützung der berechtigten Stellen umfasst somit sowohl die gerichtlich angeordneten als auch die präventiven Überwachungen.

Nach der Strafprozessordnung können höherrangige Beamte der Kriminalpolizei jeden Mitarbeiter der France Télécom sowie jeden Mitarbeiter lizenzierter Anbieter von TK-Diensten mit der technischen Durchführung einer gerichtlich angeordneten Überwachung beauftragen (Art. 11-3 c.p.p.).

Bei präventiven Überwachungen werden die Anordnungen des Premierministers den jeweiligen TK-Unternehmen zugeleitet, die dann die Maßnahme durchführen.

4.2.2 Technische Anforderungen

Grundsätzlich gilt, dass mit bestehender Technologie die Kommunikationsdaten und –inhalte überwacht werden müssen, die auf Grundlage dieser Technologie zu erhalten sind.

Für die ISP besteht keine gesetzliche Verpflichtung, technische Einrichtungen zur Sicherstellung der TK-Überwachbarkeit dauerhaft vorzuhalten. Dies schützt einen ISP nach Angaben von Experten jedoch nicht vor den Anforderungen der Behörden, permanente Einrichtungen zu installieren.

Die überwachten Daten werden der GIC – Groupement interministériel de contrôle zugeleitet, die ein Überwachungszentrum betreibt.[25] Verschlüsselte Kommunikation ist vom Anbieter dieser Kommunikationsmöglichkeit (relevant z.B. bei VPN-Anbietern) falls möglich zu entschlüsseln (Art. 11-1, Loi n° 91-636 du 10 juilliet 1991).

In der Zentrale der GIC kann die berechtigte Stelle, z.B. die Gendarmerie, die zuvor beim zuständigen Ministerium einen Antrag auf Überwachung gestellt hat (in diesem Fall wäre dies das Verteidigungsministerium), die überwachten Daten speichern oder auch live abhören.

Bei der GIC wird ein Register der Überwachungsmaßnahmen geführt, in dem nicht (mehr) benötigte Aufnahmen regelmäßig gelöscht werden.

Nach Art. 12, Loi n° 91-636 du 10 juilliet 1991 müssen Abschriften von Überwachungen vernichtet werden, sobald der Zweck, für den sie aufbewahrt wurden, entfallen ist.[26]

---

25 In der Verordnung Décret n° 2002-497 du 12 avril 2002, Décret relatif au groupement interministériel de contrôle wird die GIC erstmals offiziell erwähnt. Sie existiert jedoch bereits seit 1960, als der damalige Premierminister die administrativen Abhörsysteme der berechtigten Ministerien zu einer einzigen zusammenfasste.

26 Vgl. CNCIS (o.J.), S. 6.

4.2.3 Organisatorische Anforderungen

Anforderungen dieser Art sind in einer Verordnung festgelegt, die sowohl die berechtigten Stellen als auch die Unternehmen betrifft.[27]

Die darin allgemein formulierten Anforderungen betreffen z.B.

- die Notwendigkeit, sicherheitsüberprüftes Personal einzusetzen,
- langfristig dasselbe Personal einzusetzen (mind. 2 Jahre),
- die Anforderung, zur Kontrolle Protokolle über die Überwachung zu führen (z.B. Dauer der Maßnahme)
- sowie Geheimhaltungsvorschriften zu beachten.

4.2.4 Ausnahmen

Alle TK-Anbieter und Betreiber von TK-Anlagen sind gleichermaßen verpflichtet, die Strafverfolgungsbehörden bei der TK-Überwachung zu unterstützen. Ausnahmeregelungen hinsichtlich der Vorhaltung von technischen und organisatorischen Einrichtungen existieren nicht.

Die Überwachung von Gesprächen, die Berufsgeheimnisse von Ärzten, Anwälten, Geistlichen oder Vertretern ähnlicher Berufe betreffen, ist nach der Strafprozessordnung nicht gestattet. Die Rechte eines Anwalts der Verteidigung sind in diesem Zusammenhang umfassender geschützt und betreffen auch die TK-Überwachung als solche und nicht nur Gespräche, die mit einem jeweiligen Fall zu tun haben.[28]

4.2.5 Genehmigungsverfahren für Überwachungsvorkehrungen

Es existieren keine spezifischen Genehmigungsverfahren für technische Einrichtungen oder organisatorische Vorkehrungen.

---

27 Vgl. Décret n° 93-119 du 28 janvier 1993, Décret relatif à la désignation des agents qualifiés pour la réalisation des opérations matérielles nécessaires à la mise en place des interceptions de correspondances émises par voie de télécommunications autorisées par la loi n° 91-646 du 10 juillet 1991.

28 Vgl. Lücking, E. (1992), S. 131.

4.2.6 Von europäischen Regelungsvorgaben abweichende Regelungen

Der Europäische Gerichtshof für Menschenrechte hat mehrere Klagen gegen Frankreich wegen Missachtung des Art. 8 EMRK geführt.[29] Der Grund dafür ist in Verstößen gegen die LI-Regelungen zu suchen. In Frankreich sind Fälle von illegalen (Telefon-) Abhörmaßnahmen bekannt geworden. Es wird z.B. geschätzt, dass 1996 zahlreiche Fälle von illegalen Überwachungen, die meisten davon initiiert von Regierungsbehörden, durchgeführt worden sind.[30]

Mit dem TK-Überwachungsgesetz von 1991 ist zwar, wie vom Europäischen Gerichtshof für Menschenrechte gefordert, auch in Frankreich das Überwachen von Kommunikation auf eine rechtliche Grundlage gestellt worden, die vermuteten zahlreichen Fälle von illegal durchgeführten Maßnahmen deuten jedoch mögliche Widersprüche zwischen europäischen Regelungen und nationaler Überwachungspraxis an. Darüber hinaus ist zu betonen, dass sich die Kontrolle durch die CNCIS nur auf die präventiven Überwachungsmaßnahmen erstreckt und nicht auf gerichtlich angeordnete Maßnahmen.

4.3 Voraussetzungen für die Überwachung

4.3.1 Fälle, in denen das Überwachen der TK angeordnet werden kann

Sog. „écoutes judiciaires“ können im Fall bestimmter, schwerer Straftaten angeordnet werden und zwar bei

- Straftaten, die mit einer Freiheitsstrafe von mindestens zwei Jahren geahndet werden können.[31]

Im Gegensatz zu den Regelungen etwa in Großbritannien oder Japan ist in Frankreich die Durchführung von TK-Überwachungsmaßnahmen nicht unter Verhältnismäßigkeitsaspekten eingeschränkt, d.h. eine Verpflichtung, die Überwachungsmaßnahme als „letztes Mittel“ auszuweisen und gegen andere Beweiserhebungen abzuwägen, besteht nicht.[32] Ausnahmen für dringliche Fälle sind nicht vorgesehen.

---

29 Vgl. zu dieser Problematik im Folgenden EPIC/PI (Eds.) (2002), S. 178 sowie auch die historische Darstellung bei CNCIS (o.J.), S. 1ff.
30 Diese Behauptung wird zumindest bei EPIC/PI (Eds.) (2002), S. 178 aufgestellt.
31 Art. 100 Abs. 1 Satz 1 c.p.p.
32 In dem og. Artikel ist vielmehr festgelegt, dass eine Überwachung angeordnet werden kann „wenn die Bedürfnisse der Untersuchung sie erfordern“, zit. nach Lücking, E. (1992), S. 129.

Grundsätzlich ist die Privatsphäre durch die Verfassung und das Datenschutzrecht geschützt. Eine umfassende personenbezogene, präventive Überwachung der Telekommunikation als „interceptions de sécurité“ kann aber angeordnet werden

- im Interesse der nationalen Sicherheit oder der nationalen Verteidigung,
- bei Verdacht auf organisierten Terrorismus, Kriminalität oder Verbrechen,
- zum Schutz der französischen Wirtschaft oder Wissenschaft.[33]

Data Retention

Für die Spezifizierung der Anforderungen in Zusammenhang mit der Datenspeicherung wird zurzeit eine Verordnung erarbeitet.

4.3.2 Genehmigung einer Überwachungsmaßnahme

Überwachungsmaßnahmen – „écoutes judiciaires“ - im Rahmen der Strafverfolgung müssen von einem Untersuchungsrichter angeordnet werden. Die Anordnung wird dann dem jeweiligen TK-Unternehmen direkt zugeleitet, dass wiederum die Daten an die berechtigte Stelle ausleitet bzw. weitergibt.

Die sog. „interceptions de sécurité“ werden vom Premierminister autorisiert, und zwar auf Antrag des Innenministers, des Verteidigungsministers oder des zuständigen Ministers für Zollangelegenheiten. Diese beantragen die Überwachung auf Anforderung der ihnen nachgeordneten berechtigten Stellen (z.B. Police, Police judiciaire, Gendarmerie, DST, DGSE). Der Antrag wird zunächst der Zentralstelle GIC zugeleitet, die den Antrag zur Prüfung an die Kontrollkommission CNCIS weiterleitet.

Die Kommission gibt eine Empfehlung ab, die die GIC dem Premierminister zuleitet. Dieser unterzeichnet die Anordnung und leitet sie den jeweiligen TK-Anbietern und –Anlagebetreibern zu.

Der Premierminister ist laut Gesetz verpflichtet, innerhalb von 48 Stunden die Kontrollkommission CNCIS zu benachrichtigen. In der Praxis erfolgt diese Benachrichtigung meist früher.[34] Die Kommission verlangt ein Begleitschreiben mit ausführlicher Begründung.

Falls die Kommission die Anordnung für nicht gerechtfertigt hält, kann sie diese durch eine negative Empfehlung an den Premierminister aufhalten. Eine solche Absage wird in der Regel aufgrund einer unzureichenden Begründung oder wegen der Diskrepanz

---

33 Vgl. u.a. http://vosdroits.service-public.fr sowie Lücking, E. (1992), S. 127.
34 Vgl. CNCIS (o.J.), S. 6.

zwischen der Schwere der Vorwürfe und der Bedeutung des Fernmeldegeheimnisses erteilt.[35] Die Anzahl der Streitfälle wurde nach Angaben der CNCIS in den letzten Jahren erheblich eingeschränkt, da die berechtigten Stellen die schriftlichen Begründungen immer ausführlicher und sorgfältiger vornehmen.

Obwohl die CNCIS nur eine Empfehlung an den Premierminister aussprechen kann und dieser allein über die Durchführung der Maßnahme entscheidet, ist es in der Vergangenheit nicht vorgekommen, dass eine Überwachung entgegen der Empfehlung der Kontrollbehörde durchgeführt wurde.

4.3.3 Möglicher Zeitraum der Überwachung

Eine Überwachungsmaßnahme kann höchstens für vier Monate angeordnet und kann danach mehrfach für denselben Zeitraum erneuert werden. Eine Beschränkung besteht nicht.

Data Retention

Nach Art. 29 LSQ ist für die Speicherung von Kommunikationsdaten für Zwecke der Strafverfolgung ein Zeitraum von einem Jahr vorgesehen.

4.3.4 Überprüfung der Rechtmäßigkeit der Maßnahme durch die Verpflichteten

Es existiert keine gesetzliche Verpflichtung, die Rechtmäßigkeit der Maßnahme zu prüfen. Allerdings sieht Art. 432-9 c.p.p. vor, dass Unternehmen nur in gesetzlich legitimierten Fällen Informationen über ihre Kunden weitergeben dürfen. Bei Verstoß kann eine Geldbuße von bis zu 450.000 Euro drohen.

Vor diesem Hintergrund erscheint nach Auffassung der AFA (Association des Fournisseurs d'Accès et de Services Internet) eine Überprüfung der Anordnung im Interesse des ISP ratsam. Dies dürfte auch für die Sprachtelefonie-Anbieter zutreffen.

4.4 Durchführung der Überwachung

4.4.1 Erforderliche Angaben

In der schriftlichen Anordnung müssen jeweils enthalten sein

---

35 Vgl. ebenda.

- eine eindeutige Identifikation der Verbindung, insbesondere Name des Anschlussinhabers und seiner Anschlussnummer bzw. –kennung,
- genaue Bezeichnung der zugrundeliegenden Straftat,
- Dauer der Überwachung.

Nicht angegeben werden muss der Name der zu überwachenden Person.[36]

4.4.2 Art der zu überwachenden Telekommunikation

Das französische TK-Überwachungsgesetz aus dem Jahr 1991 bezieht ausdrücklich „jetzt und in Zukunft“ alle Arten der „Korrespondenz“ und jegliche Form „der Telekommunikationsmittel“ mit ein.[37] Dies wird von der CNCIS ausdrücklich betont.

4.4.3 Übermittlung an die berechtigten Stellen

Die Übermittlung kann in „real-time“ erfolgen, dies stellt jedoch keine Verpflichtung dar, was insbesondere für die ISP relevant ist. Sie können die abgehörten Daten online, aber auch offline an die Strafverfolgungsbehörden weitergeben.

Für die ISP gilt heute, dass sie den Anforderungen der Strafverfolgungsbehörden entsprechen, also in Echtzeit überwachte Daten ausleiten oder gespeicherte Daten weitergeben, je nach den technischen Möglichkeiten der Strafverfolgungsbehörden. In der Praxis werden die Daten in den meisten Fällen offline weitergegeben.

4.4.4 Unterschiedliche technische Einrichtungen für verschiedene Überwachungsanforderungen

An die Strafverfolgungsbehörden und die TK-Unternehmen werden strenge Anforderungen hinsichtlich der Trennung von gerichtlich angeordneten Überwachungen - „écoutes judiciaires“ - und präventiv motivierten - „interceptions de sécurité“ – gestellt. So müssen etwa die Räumlichkeiten, in denen die Abhörungen durchgeführt werden, voneinander separiert sein. Die Abhörprotokolle für eine Maßnahme dürfen außerdem nicht an andere berechtigte Stellen weitergeleitet werden.[38]

---

36 Vgl. Lücking, E. (1992), S. 135.
37 Vgl. CNCIS (o.J.), S. 8.
38 Vgl. CNCIS (o.J.), S. 7.

Für die TK-Unternehmen bestehen jedoch keine unterschiedlichen Verpflichtungen hinsichtlich technischer Einrichtungen für die Durchführung von gerichtlichen und präventiven Überwachungsmaßnahmen.

4.4.5 Echtzeit-Überwachung oder Speicherung

Die Überwachung der Sprachtelefonie erfolgt in Echtzeit und wird in „real time“ an die berechtigten Stellen übermittelt. Für Internet-Daten trifft dies nur dann zu, wenn die Strafverfolgungsbehörden entsprechend ausgestattet sind.

Data Retention

Die Regelungen bezüglich Art und Dauer der Speicherung von Kommunikationsdaten werden in der geplanten Verordnung zum LSQ weiter spezifiziert werden. Dies betrifft auch Regelungen zur Gewinnung der Daten. Die Strafverfolgungsbehörden erhalten die Daten aufgrund von Beschlagnahmungen.

Derzeit existieren folgende Selbstverpflichtungen des französischen Internetverbandes AFA über die Speicherung von Kommunikationsdaten:[39]

- Der Access-Provider speichert Login des Nutzers, zugeteilte IP-Adresse, Datum und Zeitpunkt des Beginns bzw. Endes der Verbindung, (Dauer: üblicherweise 3 Monate).
- Der Proxy-Server-Betreiber speichert IP-Adresse des Nutzers, Identifikation des angewählten Servers, angefordertes Dokument, Datum und Uhrzeit, (Dauer: üblicherweise 3 bis 5 Tage),
- Der Hosting-Provider speichert Login des Nutzers, IP-Adresse, Datum und Zeitpunkt des Beginns bzw. Endes der Verbindung, (Dauer: üblicherweise drei Monate).

Diese Daten können demnach bei Bedarf an die Strafverfolgungsbehörden innerhalb der Speicherfristen weitergegeben werden.

---

39 AFA (o.J.): Pratiques et usages des Membres de l’AFA, Paris, abrufbar unter: http://usages.afa-france.com/#conservation

4.5 Kontroll- und Sanktionsmaßnahmen

4.5.1 Kontrollinstanzen

Die Kontrolle der Einhaltung von Regeln, die die Überwachung als „interceptions de sécurité“ vorsehen, obliegt der CNCIS, der sog. Nationalen Kommission für sicherheitsbedingte Abhörmaßnahmen (Art. 13, Loi n° 91-636 du 10 juilliet 1991). Diese Kommission gibt einen jährlichen Bericht mit Daten zu Überwachungsmaßnahmen heraus, die auf Antrag der Regierung durchgeführt wurden.

Die Kommission setzt sich aus drei Mitgliedern zusammen, die von den drei höchsten Staatsvertretern nominiert werden,[40] wobei der Staatspräsident den Präsidenten der Kommission nach einem festgelegten Verfahren auswählt. Es ist üblich, dass die beiden übrigen Mitglieder jeweils der Regierungspartei bzw. der Opposition angehören. Alle Kommissionsmitglieder können während der Dauer ihrer Amtszeit nicht vorzeitig abgesetzt werden.

Zur Aufgabe der CNCIS gehört es, amtliche Kontrollvorgänge einzuleiten, auf Antrag von Privatpersonen Ermittlungen durchzuführen sowie Anfragen zu beantworten. Die Kontrollbefugnisse der Kommission konzentrieren sich auf drei Bereiche. Sie

- kontrolliert, ob die Anordnungen von dazu berechtigten Personen unterschrieben wurden,
- sie wacht über die Einhaltung der festgelegten Quoten
- und über die Legalität der Motive für die Überwachung.

Auf Antrag von Bürgern kann sie in einem konkreten Fall prüfen, ob eine Maßnahme rechtmäßig ist. Das Ergebnis wird der jeweiligen Person jedoch nicht mitgeteilt.

Die Behörde hat uneingeschränkte Zugangsbefugnis zu den Registern und technischen Einrichtungen der GIC sowie auch der TK-Unternehmen und kann somit auch vor Ort Kontrollen durchführen.

Für Überwachungsmaßnahmen aufgrund einer gerichtlichen Anordnung existieren eigene Kontrollmaßnahmen durch die jeweiligen Untersuchungsrichter, von denen die Anordnung ausgeht, sowie ggf. durch die Berufungsgerichte und den Kassationshof. Diese Kontrollen sind nicht durch das Überwachungsgesetz zentral geregelt, sondern können regionale Unterschiede aufweisen.

---

40 Dem Staatspräsidenten, dem Senatspräsidenten und dem Präsidenten der Nationalversammlung, vgl. CNCIS (o.J.).

Während die CNCIS für die Kontrolle des Umgangs mit den Kommunikationsinhalten zuständig ist, nimmt die Datenschutzbehörde CNIL (Commission nationale de l'informatique et des libertés) den Schutz von personenbezogenen Daten (Kommunikationsdaten) vor, die beispielsweise im Rahmen von Data Retention gewonnen werden.

CNCIS und CNIL sind sog. unabhängige Behörden mit Regulierungs- und Interventionsbefugnissen.

4.5.2 Berichtspflichten

Der die Überwachung durchführende Kriminalpolizeibeamte muss für jede Maßnahme ein Protokoll anfertigen, das Beginn und Ende der Maßnahme genau bezeichnet.[41]

Die Daten werden bei Überwachungsmaßnahmen aufgrund einer gerichtlichen Anordnung („écoutes judiciaires") bei den jeweiligen regionalen Gerichten in den Departements gesammelt. Sie werden jedoch nicht zu einer Gesamtstatistik zusammengeführt, so dass diesbezüglich in Frankreich keine offiziellen Daten verfügbar sind.

Angaben zur Überwachung als „interceptions de sécurité" werden an die zuständige Behörde CNCIS weitergegeben, die regelmäßig Statistiken in einem Jahresbericht veröffentlicht.

Nach Art. 16, Loi n° 91-636 du 10 juilliet 1991, sind alle Minister, öffentlichen Einrichtungen und Vertreter des öffentlichen Dienstes verpflichtet, die Arbeit der Kommission zu unterstützen. Diese Verpflichtung besteht auch für die Unternehmen.

Die interministerielle Arbeitsgruppe GIC erstattet der CNCIS jede Woche Bericht über die Aufhebung von Anordnungen und nimmt falls nötig, amtliche Aufhebungen vor, wenn die Dauer der Überwachungsmaßnahme ohne genehmigte Verlängerung überschritten wurde.[42]

---

41 Vgl. Lücking, E. (1992), S. 136.
42 Vgl. CNCIS (o.J.), S. 6.

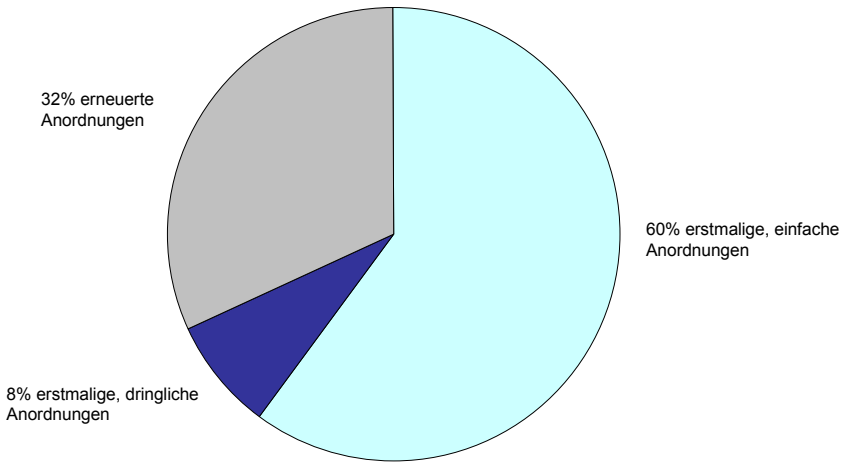
4.5.3 Statistiken

Zwischen 1997 und 2001 wurden jährlich etwa 3.000 TK-Überwachungen - „interceptions de sécurité“ - genehmigt. Im Jahr 2000 nahm die Zahl geringfügig ab. Die Überwachung von Mobiltelefonen stieg anteilsmäßig stark an. Bei etwa 10 bis 12 Prozent der Anordnungen handelt es sich um sog. dringliche Fälle.

Die Motive für Überwachungsmaßnahmen betreffen die folgenden Bereiche (vgl. Abbildung 4-1 und Abbildung 4-2 sowie Tabelle 4-1): organisiertes Verbrechen bzw. Terrorismus nimmt den wichtigsten Rang ein, darauf folgt nationale Sicherheit, danach wirtschaftliches Potenzial und Wissenschaft sowie letztendlich verbotene Gruppierungen.[43] Diese abnehmende Rangfolge hat sich seit Jahren nicht geändert.

Im Jahr 2001 wurden 4.515 präventive TK-Überwachung durchgeführt, davon wurden 3.098 erstmals angeordnet, bei 1.412 handelte es sich um Verlängerungen aus dem vorangegangenen Jahr. Im Jahr 2001 wurden 451 erstmalige Anträge bzw. Dringlichkeitsanträge abgelehnt.[44]

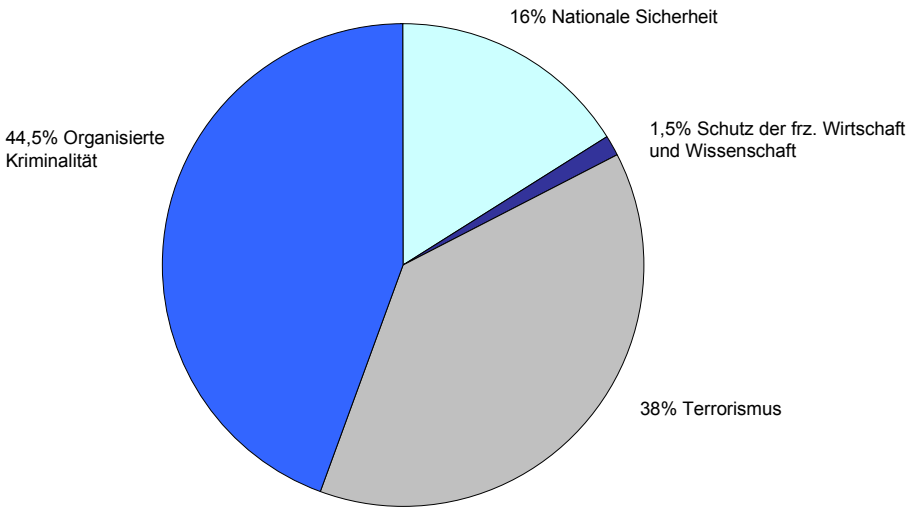
Abbildung 4-1: Verteilung nach erstmaligen und erneuerten Anträgen zur präventiven TK-Überwachung (2001)



Quelle: CNCIS 2002

43 Vgl. auch CNCIS (o.J.), S. 5.
44 Vgl. CNCIS (2002): S. 15ff.

Abbildung 4-2: Erstmalige Anträge auf präventive TK-Überwachung in 2001: Verteilung nach Motiven



Quelle: CNCIS 2002

Tabelle 4-1: Verteilung der Anträge auf präventive TK-Überwachung (1997-2001)

Anlass	1997	1998	1999	2000	2001
Nationale Sicherheit	456	491	495	449	509
Schutz der frz. Wirtschaft u. Wissenschaft	175	120	87	72	49
Terrorismus	1190	1327	1317	979	1203
Organisierte Kriminalität	1073	1124	1145	1256	1400
Verbotene Gruppierungen	7	0	0	0	0
Insgesamt	2901	3062	3044	2756	3161

Quelle: CNCIS 2002

4.5.4 Sanktionen

Die CNCIS kann folgende Maßnahmen ergreifen:[45]

- Die Behörde kann eine negative Empfehlung an den Premierminister bezüglich der Durchführung einer bestimmten Maßnahme aussprechen.
- Sie hat die Möglichkeit und Pflicht, der Gerichtsbarkeit mitzuteilen, dass eine Zuwiderhandlung gegen das TK-Überwachungsgesetz festgestellt wurde. Nur eine gerichtlich angeordnete Ermittlung kann eine illegale Abhöraktion beenden.

4.6 Kosten

4.6.1 Bewertung des Aufwands durch die Verpflichteten

Da in Frankreich die TK-Anbieter und –Anlagenbetreiber von den Behörden für die Durchführung von Überwachungsmaßnahmen vergleichsweise umfassend entschädigt werden, ist Protest – wie auch in Italien – weniger relevant innerhalb Diskussion um TK-Überwachungsmaßnahmen. Die Unternehmen können ihre tatsächlichen Kosten erstattet bekommen. Die Übertragung der Daten an die technische Zentrale der GIC wird vollständig bezahlt. Für Investitionen in technische Ausrüstung können die Unternehmen Investitionskosten geltend machen. In welcher Höhe diese erstattet werden, ist Gegenstand von Verhandlungen zwischen dem jeweiligen Unternehmen und dem jeweiligen Ministerium.

Kritik wird von den Unternehmen dahingehend geübt, dass die Kostenerstattung für TK-Überwachungsmaßnahmen langwierig und aufwändig ist.

4.6.2 Kostenübernahme und Aufwandsentschädigungen

Die netzseitigen Kosten für die von Untersuchungsrichtern angeordneten Maßnahmen trägt das Justizministerium, die für präventive Maßnahmen das Innenministerium. Diese Behörden zahlen auch für die Übermittlung der Daten an die berechtigten Stellen bzw. an die Zentrale des GIC.

---

45 Vgl. CNCIS (o.J.), S. 7.

5 Rahmenbedingungen für Lawful Interception in Italien

Die Basis der rechtlichen Bestimmungen im Bereich Lawful Interception in Italien bilden Artikel der Strafprozessordnung von 1938, die aus dem Jahr 1988 stammen. Die meisten der geltenden Regelungen unterliegen – im Unterschied zu den übrigen G7-Staaten – einer strikten Geheimhaltung.[46] Daher beschränkt sich die folgende Darstellung in erster Linie auf die Wiedergabe von Expertenaussagen.

In Italien besteht seit 1999 ein zentrales Gremium, dass die Aktivitäten auf dem Gebiet der TK-Überwachung sowie der Verbesserung der allgemeinen IT-Sicherheit koordiniert. Mitglieder der interministeriellen Gruppe, des „Komitees für Netzwerksicherheit", sind Vertreter des Innen-, Justiz- und Kommunikationsministeriums. Interessenvertreter der TK-Anbieter und –Anlagenbetreiber sind ebenfalls in die Diskussion involviert. Seit Mai 2001 liegt eine detaillierte Verordnung über die technischen und organisatorischen Verpflichtungen hinsichtlich der Sicherstellung der TK-Überwachbarkeit vor. Gleichzeitig wurde eine Regelung zur Investitionskostenerstattung für die verpflichteten Unternehmen vorgestellt.

5.1 Rechtliche Grundlagen

5.1.1 Grundlagen in der TK-Gesetzgebung

Die 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 die TK-Überwachung für Telekommunikationsnetzbetreiber und Service Provider verpflichtend ist:[47]

„13. Le prestazioni effettuate a fronte di richieste di intercettazioni e di informazioni da parte delle competenti autorità giudiziarie sono obbligatorie, non appena tecnicamente possibile da parte dell'organismo di telecomunicazioni nei tempi e nei modi che questo

---

46 Dies wird vor allem mit den Aufgaben des Staates zur Bekämpfung der organisierten Kriminalität (Mafia) begründet.

47 Diese Regelung bezieht sich nicht nur auf die Überwachung von Echtzeit-Kommunikation, sondern auch auf die Weitergabe von Kundeninformationen und Kommunikationsdatensätzen.

concorderà con le predette Autorità. Le prestazioni relative alle richieste di intercettazioni vengono remunerate secondo **un listino**, redatto per tipologie e fasce quantitative di servizi, proposto dall'organismo di telecomunicazioni ed approvato dal Ministero delle comunicazioni di concerto con il Ministero di grazia e giustizia." [Hervorhebung nicht im Original]

Das Ministerium für Kommunikation hat gemeinsam mit dem Justizministerium die in dem Dekret erwähnten Verordnungen erarbeitet, in denen die Verpflichtungen sowie die den Unternehmen zu gewährenden Entschädigungen beschrieben sind. Das Vorliegen der „listino" wurde 2001 mit einem Dekret angekündigt, in dem auch die grundsätzlichen Rahmenbedingungen für die Kostenentschädigungen festgelegt sind:

- 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, die detailliert die Anforderungen an die Unternehmen sowie die für diese Dienstleistung jeweils gewährten Kostenentschädigungen durch jeweiligen berechtigten Stellen beschreibt, ist für die betreffenden Unternehmen zugänglich, jedoch nicht für die breite Öffentlichkeit. TK-Unternehmen können die Liste beim Ministerium für Kommunikation anfordern.[48] Die Erarbeitung der technischen und organisatorischen „User Requirements" wurde ebenfalls im Mai 2001 abgeschlossen. Es ist geplant, sie den betroffenen Unternehmen in nächster Zeit zur Kenntnis zu geben, sie werden jedoch der Geheimhaltung unterliegen.

5.1.2 Einschlägige Rechtsvorschriften

Das Fernmeldegeheimnis wird in Italien durch Art. 15 der Verfassung[49] garantiert („La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili. La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge.") Einschränkungen sind nur auf Basis einer gesetzlichen Grundlage möglich. Diese werden in Italien im Rahmen des Strafrechts geschaffen. Lawful Interception ist seit 1988 in der italienischen Strafprozessordnung, Art. 266-271, geregelt:

- Intercettazioni di conversazioni o comunicazioni, Art. 266 – 271, Codice di Procedura Penale, 22. September 1988.

---

48 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). Für Forschungs- und Beratungsinstitute ist die Liste ebenfalls nicht zugänglich, es scheint jedoch für ausländische Behörden möglich zu sein, sie offiziell anzufordern.

49 Vgl. La Costituzione della Repubblica Italiana, 27 dicembre 1947. Festgelegt ist der Schutz von „Korrespondenz sowie jeder anderen Form von Kommunikation".

Die EU-Datenschutzrichtlinie 97/66/EG wurde im Frühjahr 1998 durch das Gesetz Nr. 171 vom 13. Mai 1998 umgesetzt.

- Decreto Legislativo 13 maggio 1998, n. 171, Disposizioni in materia di tutela della vita privata nel settore delle telecomunicazioni, in attuazione della direttiva 97/66/CE del Parlamento europeo e del Consiglio, ed in tema di attività giornalistica, pubblicato nella Gazzetta Ufficiale n 127 del 3 giugno 1998.

5.1.3 TK-Dienste, für die die Überwachbarkeit gewährleistet sein muss

Die einschlägigen Regelungen in der Strafprozessordnung sind technikoffen formuliert, so dass auch in Italien für alle Arten der Telekommunikation die Überwachbarkeit gewährleistet sein muss.

Data Retention

In Bezug auf die Daten, die Internet Service Provider für Zwecke der Strafverfolgung vorhalten sollen, hat sich die italienische Regierung den Forderungen der G7-Staaten angeschlossen.[50]

In Italien werden derzeit Gesetzesnovellierungen diskutiert, welche die Anforderungen der Strafverfolgungsbehörden hinsichtlich Datenspeicherung von Verkehrsdaten berücksichtigen sollen. Generell wird von der Regierung die Auffassung vertreten, dass die Dauer der Datenspeicherung um so effektiver sein wird, je länger sie gestattet ist.[51]

5.1.4 Zweck der Überwachung

Die Überwachung erfolgt zum Zweck der Strafverfolgung bei schweren Straftaten. Die Fälle, in denen eine Überwachung angeordnet werden kann, sind per Gesetz eingeschränkt.

5.1.5 Unterschiede zwischen Überwachungsmaßnahmen der Strafverfolgungsbehörden und denen der Sicherheitsbehörden

In Italien unterscheidet man wie in Frankreich zwischen individueller TK-Überwachung zur Aufdeckung einer konkreten Straftat und präventiver TK-Überwachung. Beide Arten werden von einem Richter auf Antrag des Staatsanwalts (Magistrat) angeordnet. Die

---

50 Vgl. General Secretariat of the Council (2002). Das Papier wurde von einem Abgeordneten des Europäischen Parlaments unter der folgenden Adresse im Internet veröffentlicht: http://servizi.radicalparty.org/data_retention/index.htm.

51 Vgl. ebenda.

Ergebnisse der präventiven TK-Überwachung können vor Gericht nicht als Beweis verwendet werden und müssen 5 Tage nach Ende der Maßnahme vernichtet werden.

5.2 Verpflichtungen für die TK-Anbieter und Betreiber von TK-Anlagen

5.2.1 Kreis der Verpflichteten

Alle Netzbetreiber und Service Provider sind nach dem Decreto del presidente della repubblica del 19 settembre 1997, n. 318, verpflichtet, die Überwachbarkeit der Telekommunikation zu gewährleisten. Dazu haben sie technische Einrichtungen vorzuhalten und organisatorische Vorkehrungen zu treffen.

5.2.2 Technische Anforderungen

Seit Mai 2001 bestehen detaillierte technische Anforderungen, die die Basis für die „listino“ bilden, welche die Höhe der Kostenentschädigungen für die Verpflichteten enthält. Die Anforderungen werden demnächst den betroffenen Unternehmen zur Kenntnis gebracht werden. Sie unterliegen jedoch einer strikten Geheimhaltung.

Es existieren unterschiedliche Vorschriften für die Anbieter folgender Sprach- und Daten-Dienste:

- drahtgebundene Dienste,
- mobile Dienste,
- Satellitendienste,
- Long-distance Calls,
- International Calls.

Alle diese Unternehmen müssen technische Einrichtungen und organisatorische Vorkehrungen permanent vorhalten.

Zurzeit existiert noch keine Spezifikation für die ISP, d.h. für die Überwachung von E-Mail und anderen Internetdiensten. Eine solche Regelung befindet sich in Vorbereitung. Voraussichtlich wird sie im Sommer 2003 vorgelegt werden.

5.2.3 Organisatorische Anforderungen

Seit Mai 2001 bestehen auch detaillierte organisatorische Anforderungen, die demnächst den betroffenen Unternehmen zur Kenntnis gebracht werden. Sie unterliegen jedoch einer strikten Geheimhaltung.

5.2.4 Ausnahmen

Es bestehen derzeit keine Ausnahmen in Bezug auf die Vorhalteverpflichtungen, diese erscheinen jedoch künftig für kleinere ISP denkbar.

Die Überwachung der Telekommunikation von Personen mit einem religiösen Amt, Rechtsanwälten, Ärzten und Personen mit anderen, sensitiven Berufen, die Verschwiegenheitspflichten unterliegen, ist nicht gestattet. Ausnahmen existieren für Anti-Mafia-Fälle.[52]

5.2.5 Genehmigungsverfahren für Überwachungsvorkehrungen

Die Regelung beruht auf einer Selbstkontrolle durch die TK-Unternehmen. Jedes TK-Unternehmen legt bei Aufnahme der Geschäftstätigkeit auf Grundlage der vorgesehenen Genehmigung (Lizenz oder Autorisierung) eine Erklärung vor, in der es sich verpflichtet, die notwendigen Vorkehrungen zur Sicherstellung der Überwachbarkeit der Telekommunikation zu treffen.[53]

5.2.6 Von europäischen Regelungsvorgaben abweichende Regelungen

Die Richtlinie 97/66/EG wurde vollständig in die italienische Gesetzgebung aufgenommen, so dass man diesbezüglich derzeit nicht von einer Kollision mit EU-Vorgaben sprechen kann. Die Umsetzung der aktuellen EU-Datenschutzrichtlinie 2002/58/EG steht noch aus. Im Rahmen dieser Implementation können auch die Pläne zur Datenspeicherung EU-konform umgesetzt werden.

---

52 Vgl. EPIC/PI (Eds.) (2002), S. 232.
53 Derzeit sind in Italien ca. 190 Lizenzinhaber und ca. 4.000 autorisierte Unternehmen am Markt.

5.3 Voraussetzungen für die Überwachung

5.3.1 Fälle, in denen das Überwachen der TK angeordnet werden kann

Die Überwachung der Telekommunikation kann bei Verdacht auf die folgenden Straftaten erfolgen:[54]

- Straftaten, die eine lebenslängliche oder eine Freiheitsstrafe von mindestens 5 Jahren nach sich ziehen,
- Straftaten gegen den Staat, die eine Freiheitsstrafe von mindestens 5 Jahren nach sich ziehen,
- Straftaten im Zusammenhang mit Drogen-, Waffen-, Sprengstoffhandel oder Schmuggel,
- Beleidigung, Bedrohung, Belästigung, Verfolgung o.ä. mittels Telefonie.

5.3.2 Genehmigung einer Überwachungsmaßnahme

Eine Überwachung der Telekommunikation nach der Strafprozessordnung darf nur erfolgen, wenn eine gerichtliche Anordnung auf Antrag eines Staatsanwalts – des sog. Magistrats - vorliegt.

In dringenden Fällen kann der Staatsanwalt die Überwachung anordnen; es ist eine Bestätigung durch den Richter im Nachhinein erforderlich.

Data Retention

Gespeicherte Kommunikationsdaten und -inhalte können ebenfalls im Rahmen einer Anordnung auf Herausgabe bzw. einer Beschlagnahmung von den Strafverfolgungsbehörden angefordert werden.

In der Anordnung wird festgelegt, ob eine Übergabe oder Beschlagnahmung der Daten stattfindet. Die Durchführung nimmt die Gerichtspolizei vor, welche die Anordnung dem jeweils betroffenen TK-Anbieter bzw. Betreiber von TK-Anlagen übergibt.

Der Prozessablauf im Bereich Lawful Interception und Data Retention wird als unproblematisch und effektiv wahrgenommen.[55]

---

54 Vgl. ebenda.
55 Vgl. General Secretariat of the Council (2002).

5.3.3 Möglicher Zeitraum der Überwachung

Eine Überwachungsmaßnahme kann für 15 Tage angeordnet und kann für denselben Zeitraum durch einen Richter verlängert werden. Sie sollte nicht öfter als drei Mal verlängert werden, es gibt jedoch Fälle, wo dies für erforderlich gehalten wurde.

In sog. Mafia-Strafverfolgungsverfahren kann eine Überwachung für 40 Tage angeordnet und noch einmal für 20 Tage durch einen Richter eines der 26 District Anti-Mafia-Directions verlängert werden. Auch in diese Maßnahmen sollten nicht häufiger als drei Mal verlängert werden, es existieren jedoch Fälle, wo dies notwendig war.

5.3.4 Überprüfung der Rechtmäßigkeit der Maßnahme durch die Verpflichteten

Eine solche Verpflichtung besteht nicht. Den TK-Unternehmen wird nicht ein Original der Anordnung übergeben, sondern nur eine Erklärung der berechtigten Stelle, dass eine solche vorliegt.

Von Bedeutung für die Unternehmen ist jedoch in ihrem eigenen Interesse wie in anderen G7-Staaten auch die rechtmäßige und kontrollierte Durchführung der Überwachungsmaßnahme im Unternehmen. Dazu führen die Unternehmen interne Kontrollmaßnahmen durch.

5.4 Durchführung der Überwachung

5.4.1 Erforderliche Angaben

In der Anordnung muss der zu überwachende Anschluss spezifiziert werden. Bei der Festnetztelefonie geschieht dies durch die Teilnehmerrufnummer (Telefonnummer). Im Mobilfunk erfolgt die Spezifizierung durch die Teilnehmerrufnummer (MSISDN oder Telefonnummer), durch die International Mobile Subscriber Identity (IMSI) und durch die International Mobile Equipment Identity (IMEI). In der Internetkommunikation wird der zu überwachende Anschluss durch die Teilnehmerkennung und den Benutzernamen gewährleistet.

5.4.2 Art der zu überwachenden Telekommunikation

Es muss eine exakte Kopie der transferierten Daten vorliegen, da laut Gesetz in einem Verfahren dem Strafverteidiger ein „Original“ der abgehörten Daten zugänglich gemacht werden muss. Daher müssen die „Rohdaten“ ausgeleitet werden.

Für Voice over IP gilt, dass auf diesen Dienst dieselben Regelungen wie in der Sprachtelefonie angewendet werden und somit die Sprache an die berechtigten Stellen übermittelt werden muss.

5.4.3 Übermittlung an die berechtigten Stellen

Inhalt und Kommunikationsdaten der zu überwachenden Kommunikation sind in „real time“ an die berechtigten Stellen zu übermitteln.

Internet-Kommunikation wird im Beisein eines Beamten der berechtigten Stelle auf CD-ROM gespeichert und übergeben. Geplant ist jedoch auch hier eine „real time“-Übermittlung.

Unterschiedliche Überwachungsanordnungen müssen getrennt behandelt werden, ohne dass eine Stelle von der anderen Kenntnis erlangt. Die überwachte Kommunikation muss der jeweiligen berechtigten Stelle direkt zugeleitet werden. Es existiert demnach keine zentrale technische Einrichtung der berechtigten Stellen wie etwa in Frankreich.

5.4.4 Unterschiedliche technische Einrichtungen für verschiedene Überwachungsanforderungen

Es besteht keine Notwendigkeit, die Unternehmen für die Durchführung von gerichtlich angeordneten oder präventiven Überwachungsmaßnahmen zur Vorhaltung unterschiedlicher technischer Einrichtungen zu verpflichten.

5.4.5 Echtzeit-Überwachung oder Speicherung

Die Telekommunikation muss in Echtzeit überwacht werden und in „real time“ an die jeweilige berechtigte Stelle übermittelt werden. Eine Ausnahme sind die Verpflichtungen für die nationalen Long-distance Carrier. Diese sind nicht zur Vorhaltung von Echtzeit-Monitoring-Systemen verpflichtet.[56]

Data Retention

Kommunikationsdatensätze sollen länger als 8 Monate gespeichert werden. Welche Datensätze von den ISP gespeichert werden müssen, ist noch nicht abschließend geklärt und ist Gegenstand der derzeitigen Diskussion.

Rechnungsdaten dürfen in Italien für 5 Jahre gespeichert werden.

---

56 Diese Kommunikation wird im Teilnehmeranschlussbereich von den verpflichteten Anbietern, die „drahtgebundene“ Kommunikation anbieten, abgedeckt.

5.5 Kontroll- und Sanktionsmaßnahmen

5.5.1 Kontrollinstanzen

Der Richter, der die Anordnung zur Überwachung erlässt, kontrolliert auch die Einhaltung der Vorschriften für die Aufbewahrung der Aufnahmen der Telekommunikation bzw. deren Transskription. Alle Daten, die nicht für den bestimmten Zweck der Strafverfolgung benötigt werden, müssen zerstört werden.[57]

5.5.2 Berichtspflichten

Es erfolgen Zählungen durch das Justizministerium, die aber nicht veröffentlicht werden.

5.5.3 Statistiken

Es existieren Schätzungen über den Umfang der Überwachung. Für das Jahr 1996 belaufen sich diese nach Ansicht der Organisation EPIC auf 44.000 überwachte Kennungen, 1992 sollen es nur 15.000 gewesen sein.[58]

5.5.4 Sanktionen

Sanktionen bestehen nur im Rahmen der allgemeinen Strafgesetzgebung. In den erwähnten einschlägigen Regelungen sind keine Sanktionen festgelegt.

5.6 Kosten

5.6.1 Bewertung des Aufwands durch die Verpflichteten

Auch in Italien wird der Aufwand für die Überwachung von den Unternehmen als erheblich eingestuft. Da jedoch eine Lösung zur Kostenentschädigung gefunden wurde, die einen wesentlichen Teil der Kosten abdeckt, ist der Protest in Bezug auf die technischen und organisatorischen Verpflichtungen zurückhaltend.

---

57 Vgl. EPIC/PI (Eds.) (2002), S. 232.

58 Vgl. EPIC/PI (Eds.) (2002), S. 232. Zum Vergleich: In Italien leben 57,7 Mio. Menschen. Da keine Angaben zur Quelle gemacht werden, ist diese Statistik kaum als seriöse Schätzung zu bewerten.

Die interministerielle Arbeitsgruppe des Kommunikations-, Justiz- und des Innenministeriums setzt sich mit diesem Thema weiterhin in Bezug auf eine Regelung für die ISP auseinander. Der italienische Internet-Provider-Verband ist in die Beratungen eingebunden. Die ISP befürchten wie in anderen Staaten auch hohe Kosten auf Grund der Anforderungen der Strafverfolgungsbehörden zur Datenspeicherung und Internet-Überwachung im Zusammenhang mit der Bekämpfung des internationalen Terrorismus sowie der organisierten Kriminalität.

5.6.2 Kostenübernahme und Aufwandsentschädigungen

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.

Das Konzept sieht folgende Stufen der Kostenentschädigung vor:

- „Rates for the past“: Unternehmen, die vor dem 31.12.2001 in Überwachungstechnik investiert haben, erhalten den höchsten Satz, da sie noch nicht entsprechend der Anforderungen der berechtigten Stellen ihren Netzausbau effizient planen konnten. (Die Sätze entsprechen etwa 65% bis 50% der ursprünglich von den Unternehmen geforderten Erstattungshöhe.)

- „Rates for the future“: Unternehmen, die vom 1.01.2002 bis 31.12.2004 in Überwachungstechnik investieren, erhalten geringere Kostenentschädigungen, da sie bereits nach dem jetzt geltenden Dekret planen, so die Möglichkeit haben, effizient zu agieren und dementsprechend ihre Kosten für LI senken können. (Die Sätze entsprechen weniger als 50% der Unternehmensforderungen.) Die Unternehmen haben sechs Monate Zeit, ihre Prozesse gemäß der Forderungen zu optimieren.

- „Operational Cost Rates“: Unternehmen, die nach dem 1.01.2005 Überwachungstechnik beschaffen, können keine Investitions-, sondern nur noch Übertragungs- und Personalkosten geltend machen, da sie bereits seit drei Jahren von den Forderungen der „listino“ Kenntnis haben und ihre Planungen entsprechend ausrichten konnten. (Die Sätze entsprechen weniger als 35% der Forderungen.)

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

6 Rahmenbedingungen für Lawful Interception im Vereinigten Königreich

Die Diskussion über Überwachungsmaßnahmen und Datenspeicherung spitzt sich im Vereinigten Königreich momentan zu. Der öffentliche Protest und die kontroverse Diskussion des Themas im House of Commons und House of Lords hat dazu geführt, dass das im Jahr 2000 verabschiedete Gesetz Regulation of Investigatory Powers Act (RIPA) neu überdacht wird. Teile des Gesetzes konnten nicht wie geplant in Kraft treten, u.a. sind davon Regelungen zu Data Retention betroffen. Die Akteure warten nun auf die Initiierung eines neuen Konsultationsprozesses durch die Regierung, der für die Zeit nach der offiziellen Parlamentseröffnung im November 2002 geplant ist. Dieser Prozess wird erfahrungsgemäß etwa drei Monate in Anspruch nehmen. Es wird damit gerechnet, dass dann viele Einzelfragen neu diskutiert werden müssen und die Lösung dieser Details Auswirkungen auf die Auslegung des RIPA haben wird.

Die Situation wird derzeit als äußerst problematisch von den Akteuren wahrgenommen:

- Entscheidende Teile des neuen Gesetzes, die das Überwachen von Telekommunikation im Allgemeinen – über Sprachtelefonie hinaus – ermöglichen, sind in Kraft, es fehlen jedoch noch wichtige, präzisierende Verordnungen (Codes of Practice, Handbücher zu technischen Anforderungen u.ä.).

- Regelungen zu Data Retention sollen zunächst auf Basis von freiwilligen Vereinbarungen zwischen Strafverfolgungsbehörden und Industrie ermöglicht werden. Eine solche Vorgehensweise würde jedoch nach Auffassung von Juristen gegen die EU-Regelungen verstoßen, wonach solche Bestimmungen nur dann legal sind, wenn sie auf einer gesetzlichen Grundlage beruhen.

- Darüber hinaus ist eine Ausweitung der Befugnisse im Bereich der Datengewinnung vorgesehen, insbesondere was die Anzahl der berechtigten Stellen und eine vereinfachte Genehmigung von Maßnahmen betrifft. Die betreffenden Verordnungsvorschläge der Regierung sind auf massiven Protest gestoßen und mussten zurückgezogen werden.

6.1 Rechtliche Grundlagen

6.1.1 Grundlagen in der TK-Gesetzgebung

Im Telecommunications Act 1984 (ergänzt durch die Telecommunications Regulations 1999), der sich zurzeit in einem Novellierungsprozess befindet sowie in den diversen Regelungen des Radiocommunications Act und auch z.B. des Wireless Telegraphy Act 1949 sind Belange des Lawful Interception berührt. Die diesbezüglichen Bestimmungen

in den jeweiligen Lizenzen der Netzbetreiber wurden durch die jüngste RIPA-Gesetzgebung in diesem Bereich ersetzt.[59]

Datenschutzbestimmungen in diesem Zusammenhang finden sich außer im Human Rights Act 1998, im Data Protection Act 1998 und in den Telecommunications (Data Protection and Privacy) Regulations 2000 auch im Rehabilitation of Offenders Act 1974, Police Act 1997, Broadcasting Act 1996, Protection from Harassment Act 1997, Police and Criminal Evidence Act 1984, Crime and Disorder Act 1998 sowie in der Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 und weiteren Regelungen.[60]

Es muss an dieser Stelle darauf verzichtet werden, die komplexen Zusammenhänge im Rechtssystem des „Common Law“[61] im Vereinigten Königreich im Einzelnen zu erläutern. Da auf dem Gebiet des Lawful Interception eigene Gesetze und Verordnungen erlassen wurden, wird im Folgenden ausschließlich auf diese Kernbereiche Bezug genommen und nur für wichtige Bereiche des Datenschutzes auf die entsprechenden korrespondierenden Regelungen hingewiesen.

6.1.2 Einschlägige Rechtsvorschriften

Einschlägig für die Regelung von Lawful Interception im Vereinigten Königreich ist das im Jahr 2000 verabschiedete Gesetz über Ermittlungsbefugnisse „Regulation of Investigatory Powers Act 2000“ (RIPA). In dem Gesetz sind Anlässe für Abhörmaßnahmen sowie die Verfahren selbst geregelt. Es fällt in den Zuständigkeitsbereich des Innenministeriums (Home Office). Ein Teil des Gesetzes stellt faktisch eine Novellierung des Interception of Communications Act 1985 (IOCA) dar, und wurde u.a. deshalb verabschiedet, um den neuen technischen Entwicklungen der Telekommunikation und den damit einhergehenden Erfordernissen der Strafverfolgungsbehörden Rechnung zu tragen.[62]

RIPA besteht aus den folgenden Teilen:

- Part I Chapter I „Interception“: Dieser Teil betrifft Überwachungsmaßnahmen der Telekommunikation im engeren Sinne und stellt die faktische Novellierung des IOCA dar.

---

59 Das Vereinigte Königreich besitzt kein Strafgesetzbuch („Criminal Code“).

60 Vgl. EPIC/PI (Eds.) (2002), S. 379.

61 Das Fallrecht („Common Law“) steht im Gegensatz zum beispielsweise in Deutschland implementierten Rechtssystem des sog. „Civil Law“, des kodifizierten Rechts. Es wird u.a. deshalb von Rechtsexperten als problematisch im Bereich LI bewertet, weil verschiedene diesbezügliche Regelungen (z.B. in Bezug auf TK-Recht, Datenschutzrecht) nebeneinander stehen und z.T. unklar ist, welche Regelung vorrangig zu befolgen ist.

62 IOCA wurde 1985 deshalb initiiert, weil es notwendig war, den Erfordernissen der EU nach einer *gesetzlichen* Regelung von Lawful Interception zu entsprechen. Zuvor war die Überwachung der Telekommunikation eine gängige, jedoch nicht gesetzlich legitimierte, Praxis.

- Part I Chapter II „Acquisition and Disclosure of Communications Data“: Dieser Teil stellt eine Ausweitung der Überwachungsmaßnahmen im Hinblick auf Data Retention dar. Er betrifft die Gewinnung und Weitergabe von Kommunikationsdaten an die Strafverfolgungsbehörden im Sinne von Nutzungsdaten (Traffic Data),[63] d.h. jegliche Daten, welche die Begleitumstände einer Kommunikation betreffen.[64] Er ist auf Grund von Protesten im Parlament und bei den betroffenen Akteuren noch nicht in Kraft. Dieser Schritt ist anvisiert für März 2003. Ob der Zeitplan eingehalten werden kann, erscheint angesichts der kontroversen öffentlichen Diskussion fraglich.

- Part II regelt die Durchführung von Überwachungsmaßnahmen – strategische („general“) und individuelle („directed“) – die über den Bereich Telekommunikation hinausgehen (z.B. Überwachung von Wohnungen, Fahrzeugen) bzw. in den Aufgabenbereich der Geheimdienste fallen. Part III des Gesetzes beinhaltet eine Krypto-Regelung mit eingeschränktem Escrow-System. Part IV regelt Prüfungen und Kontrollen in Bezug auf die Einhaltung der gesetzlichen Vorgaben.

Zur Erläuterung des Ablaufs von Abhörmaßnahmen sowie der Verpflichtungen und Rechte der Strafverfolgungsbehörden hat das Innenministerium für die Behörden einen Code of Practice veröffentlicht, der auch für die verpflichteten Post- und TK-Unternehmen als Informationsquelle dient.[65]

Die Verpflichtungen der Unternehmen über das Vorhalten von Abhörtechnik sind in einer Verordnung festgelegt.[66]

Die Einhaltung des RIPA im Bereich Überwachung (Part I) wird vom Interception of Communications Commissioner kontrolliert, der dem Premierminister jährlich Bericht erstattet. Der Bericht wird in Teilen veröffentlicht und liegt für 2000 und 2001 bereits vor.

Das National Technical Assistance Centre (NTAC) fungiert als technisches Beratungszentrum für die berechtigten Stellen und ist für sie Ansprechpartner für alle Fragen in Bezug auf Lawful Interception. Es soll überdies das geplante Key-Escrow-System implementieren.

---

63 Gemeint sind auch Reverse-Funktionen für die Suche nach TK-Adressen (z.B. Telefonnummern) sowie geographische Daten (z.B. Standortdaten in der Mobilkommunikation).

64 Im folgenden wird dennoch auf diese Regelungen Bezug genommen, da zu erwarten ist, dass sie demnächst in dieser Form in Kraft treten.

65 Home Office (Hrsg.) (2002): Interception of Communications. Code of Practice. Pursuant to Section 71 of the Regulation of Investigatory Powers Act 2000. Wie im gesamten Bericht wird auch in diesem Kapitel darauf verzichtet, näher auf die Verpflichtungen der Postunternehmen bezüglich LI einzugehen.

66 The Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002.

Data Retention und Datenschutz[67]

Data Retention-Regelungen finden sich außerdem in dem nach dem 11. September 2001 initiierten Gesetz zur Terrorismus-Bekämpfung. Dazu wurde im Jahr 2001 der „Anti-terrorism Crime and Security Act (ACSA)“[68] in Kraft gesetzt. Teil 3 des Gesetzes beschäftigt sich mit „Disclosure of Information“ und Teil 11 mit dem aktuellen Thema Data Retention („Retention of Communications Data“).

Datenschutzbelange sind durch den Data Protection Act 1998 geregelt, welcher die EU-Datenschutzrichtlinie 97/66/EG umfassend umsetzt. Dort heißt es, dass das Datenschutzrecht unter allen Umständen gewahrt werden muss (ACSA, Part 3, Sec. 19 (7)), d.h. Daten, deren Veröffentlichung durch dieses Gesetz verboten ist, dürfen auch nicht im Rahmen der TK-Überwachungsgesetzgebung veröffentlicht werden.

Im Anti-Terrorismus-Gesetz ist vorgesehen, dass der zuständige Secretary of State, d.h. der Innenminister, eine Verordnung (Code of Practice) erlässt, in der die Datenspeicherung geregelt ist (Part 11, Sec. 102 (1)). Dieser Kodex wird zur Zeit unter Federführung des Innenministeriums unter Konsultierung des Information Commissioner,[69] weiterer Ressorts, der Strafverfolgungsbehörden sowie der Industrie erarbeitet. Geplant ist eine freiwillige Übereinkunft.

Der prozessuale Ablauf einer Überwachungsmaßnahme in Zusammenhang mit dem o.g. Gesetz ist in einer Richtlinie festgehalten, die von der Association of Chief Police Officers und HM Customs and Excise[70] erarbeitet wurde. Dieses nicht-öffentliche „Manual of Standards for Accessing Communications Data“ beschreibt die Verfahren zur Datengewinnung bei der Strafverfolgung sowie die korrespondierende Gesetzgebung. Zwischen der Industrie und den Strafverfolgungsbehörden bestehen Arbeitsabkommen (Working Agreements) über die Durchführung von Maßnahmen.

Die dieses Gesetz betreffenden Vereinbarungen und Verordnungsentwürfe sind unserer Kenntnis nach nicht öffentlich zugänglich. Der oben erwähnte Weg, Daten auf freiwilliger Basis den Strafverfolgungsbehörden zur Verfügung zu stellen, ist rechtlich äußerst umstritten. Es wird die Auffassung vertreten, dass nur das Schaffen einer gesetzliche Grundlage in diesem Bereich zulässig ist und in Übereinstimmung mit den EU-Anforderungen sowie der Datenschutzgesetzgebung steht.

Weitere Gesetzesgrundlagen

Der Human Rights Act 1998 setzt die Europäischen Menschenrechtskonvention (EMRK) um, insbesondere im Hinblick auf die Gewährleistung der Privatsphäre. Die

---

67 Vgl. zu den Angaben in diesem Abschnitt General Secretariat of the Council (2002).
68 Anti-terrorism, Crime and Security Act 2001, 2001 Chapter 24, Act of Parliament [United Kingdom]
69 Vergleichbar mit der Funktion des deutschen Bundesdatenschutzbeauftragten.
70 Verband der Polizeipräsidien und die Behörde Ihrer Majestät für Zoll und indirekte Steuern

Verabschiedung eines Gesetzes über die Menschenrechte war im Vereinigten Königreich deshalb notwendig, weil das Land nicht über eine geschriebene Verfassung verfügt, die diese Rechte kodifiziert. In RIPA wird auf den Human Rights Act 1998 Bezug genommen. Das TK-Überwachungsgesetz trägt somit den Anforderungen an die Wahrung der Privatsphäre und den Datenschutz Rechnung.

6.1.3 TK-Dienste, für die die Überwachbarkeit gewährleistet sein muss

Eine Anordnung nach RIPA ergeht zur Überwachung einer bestimmten Person, nicht einer Adresse oder Telefonnummer, wie dies unter dem vorhergehenden Gesetz (IOCA 1985) geregelt war. Zur Spezifizierung einer kommunikationsbezogenen Überwachungsmaßnahmen ist es jedoch notwendig, Adressen, Nummern oder Apparate, die überwacht werden sollen, in der Anordnung näher zu bezeichnen (RIPA Sec. 8 (2)).

Der Vorteil der Anordnung der Überwachung von Personen liegt nach Auffassung der Befürworter des Gesetzes darin, dass alle Kommunikationsvorgänge der Person erfasst werden können. E-Mail und Pager-Nachrichten konnten beispielsweise unter dem vorhergehenden Gesetz nicht berücksichtigt werden.

Wird die Überwachung über den zunächst beantragten Zeitraum von bis zu drei Monaten fortgesetzt, ist nur *eine* Verlängerung – bezogen auf die Person, nicht auf jede einzelne Kennung - erforderlich. Dies vermindert den Verwaltungsaufwand. Verlängerungen können für weitere drei Monate (bei schweren Straftaten) und sechs Monate (bei Gefährdung der nationalen Sicherheit und des wirtschaftlichen Wohlergehens) erfolgen; eine Obergrenze für die Anzahl der Verlängerungen besteht nicht.

6.1.4 Zweck der Überwachung

Grundsätzlich gilt im Vereinigten Königreich, dass die Möglichkeit der Überwachung nicht Grundlage im Ermittlungsverfahren sein darf und dass die bei Überwachungen gewonnenen Daten bei Gerichtsverfahren nicht verwertet werden dürfen (RIPA Sec. 17). Weder die Anklage noch die Verteidigung dürfen von diesem Material Gebrauch machen. Ausnahmen sind genauestens geregelt und betreffen die Erlaubnis, in bestimmten Fällen bei einer strafrechtlichen Verfolgung die erhobenen Daten zu verwenden. Der Staatsanwalt darf in diesen Fällen Kenntnis von dem Material erlangen, es jedoch nicht zu Zwecken einsetzen, die eine faire gerichtliche Verhandlung gefährden. Ein Richter kann in wenigen Ausnahmefällen Einblick in die Überwachungsdaten verlangen, wenn dies für den Fortgang einer Gerichtsverhandlung sinnvoll erscheint.

6.1.5 Unterschiede zwischen individuellen Überwachungsmaßnahmen der Strafverfolgungsbehörden und denen der Sicherheitsbehörden sowie strategischer Überwachung

Die Trennung nach individueller und strategischer Überwachung (strategische („general“) und gezielte („directed“) surveillance) ist in RIPA Part II enthalten. Dieser Teil des Gesetzes betrifft die allgemeine Überwachung von Personen.[71]

Die Formulare, mit denen Strafverfolgungs- und Sicherheitsbehörden diese *individuellen* Überwachungsmaßnahmen beantragen müssen, sind online von der Homepage des Innenministeriums abrufbar und geben Aufschluss über die in diesem Zusammenhang erforderlichen Angaben. Besonderes Gewicht liegt auf der Begründung, warum Daten nicht auf andere Weise beschafft werden können und ob die Verhältnismäßigkeit gewahrt bleibt, d.h. z.B. im Hinblick auf Schutz der Privatsphäre und auch im Hinblick auf mit der Überwachung verbundenen Kosten. Das bedeutet, dass in einem Antrag auf Überwachung folgende Angaben ausreichend sind:[72]

- Name der zu überwachenden Person,
- Adresse,
- Geburtsdatum.

Im Antrag auf Überwachung muss u.a. enthalten sein:

- der Zweck der Überwachung,
- zutreffende Begründung nach Sec. 28(3) of RIPA,
- Begründung für die Überwachung,
- Begründung der Verhältnismäßigkeit,
- Beschreibung der Art der Überwachung (z.B. Überwachung von Gebäuden, Fahrzeugen),
- Beschreibung, welche Information Ergebnis der Überwachung sein soll,
- Beschreibung/Begründung möglicher Rechtsverletzungen Dritter,
- Zeitraum der Überwachung.

---

71 Für diesen Bereich wurden zwei Code of Practice verabschiedet: Covert Human Intelligence Sources, Code of Practice, Pursuant to Section 71 of the RIPA 2000 und Covert Surveillance, Code of Practice.

72 Vgl. die unter http://www.homeoffice.gov.uk/ripa/p2forms.htm abrufbaren Formulare.

Strategische Überwachung in der Telekommunikation ist in RIPA Sec. 8 (4) und (5) geregelt. Dort heißt es sinngemäß, dass zur Überwachung von Kommunikation mit dem Ausland keine spezifischen Angaben zu der zu überwachenden Person bzw. deren TK-Anschlüssen enthalten muss, dies bedeutet, dass strategische Überwachung mittels Suchbegriffen o.ä. möglich ist. Experten vermuten, dass dazu TK-Unternehmen zusätzliche, spezifische technische Vorrichtungen bereithalten müssen. Dazu existieren jedoch keine veröffentlichten Bestimmungen.

6.2 Verpflichtungen für die TK-Anbieter und Betreiber von TK-Anlagen

6.2.1 Kreis der Verpflichteten

RIPA verpflichtet die „Communications Service Provider (CSP)“, die berechtigten Stellen bei der Durchführung von Abhörmaßnahmen zu unterstützen. Unter CSP sind alle diejenigen Unternehmen zu verstehen, die einen öffentlichen TK-Dienst anbieten. Dabei muss es sich nicht um ein Angebot mit Gewinnerzielungsabsicht handeln. Diese Anbieter bzw. Betreiber fallen unter die Regelungen des Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002, eine Verordnung des Innenministeriums, die in ihrer Ausrichtung mit der deutschen TKÜV vergleichbar ist und seit 1. August 2002 Gültigkeit besitzt.[73] Für Regelungen bezüglich Data Retention liegen noch keine Regelungen vor.

Die Verordnung sieht vor, dass der Innenminister jeden aus seiner Sicht relevanten Anbieter darüber informiert, welche Anforderungen zur Sicherstellung der Überwachbarkeit der Telekommunikation an ihn gestellt werden („Notice“).[74] Einer solchen Mitteilung soll ein Informationsgespräch zwischen Regierung und dem CSP vorausgehen. Der CSP kann sich zum Zweck der Konsultation an ein technisches Beratungsgremium wenden (Technical Advisory Board), wenn er die Anforderungen, die in der Mitteilung gestellt werden, für unverhältnismäßig hält.

Es liegen noch keine Erfahrungen mit dem Board vor, da es bisher nur einmal zu einer konstituierenden Sitzung zusammengetreten ist und noch keine vermittelnden Tätigkeiten aufgenommen hat. Es setzt sich aus sechs Vertretern der berechtigten Stellen und sechs Vertretern der Industrie sowie einem unabhängigen Vorsitzenden zusammen. Da von Seiten der Behörden nur Juristen und keine Technikexperten nominiert wurden, wird die Effektivität des Gremiums von Seiten der Industrie angezweifelt.

---

73 Die Ausführungen in diesem und den folgenden (Unter-)Kapiteln beziehen sich, wenn nicht anders angegeben, auf diese Verordnung.

74 Die Liste der CSP, die eine solche Mitteilung erhalten haben, ist vertraulich. Es ist davon auszugehen, dass allen größeren Anbietern eine „Notice“ zugestellt werden wird.

Grundsätzlich sind nach RIPA (Sec. 11 (5)) nur solche Unterstützungsleistungen vom CSP zu erbringen, die „vernünftigerweise“ durchführbar sind. Was dies im Einzelnen im Hinblick auf die Gewährleistung der Verhältnismäßigkeit heißt, ist zwischen den verpflichteten Unternehmen und der Regierung zu vereinbaren.

6.2.2 Technische Anforderungen

Die Anbieter von TK-Diensten und Betreiber von TK-Anlagen sind verpflichtet,[75]

- die Überwachung der gesamten Telekommunikation und der damit verbundenen Kommunikationsdaten sicherzustellen und diese Daten so zeitnah wie möglich („in near real time“) an einen Übertragungspunkt des TK-Anbieters bzw. -Anlagenbetreibers weiterzuleiten, der mit der jeweiligen berechtigten Stelle vereinbart wurde,

- die Übertragung der Daten so zu gewährleisten, dass Inhalt und Begleitumstände der Kommunikation eindeutig zuzuordnen sind,

- sicher zu stellen, dass die Übertragungsschnittstelle den Anforderungen des Innenministeriums entspricht, welche mit den üblichen internationalen Standards (wie sie von ETSI[76] beschrieben werden) übereinstimmt,

- die Daten so zu filtern, dass nur die Nutzungsdaten des jeweils zu Überwachenden weitergeleitet werden,

- zu gewährleisten, dass den berechtigten Stellen Inhalt und Begleitumstände der Kommunikation in Klarform zugänglich sind (d.h. dass ggf. Verschlüsselungen, wie sie z.B. VPN bieten, entfernt werden müssen),

- die simultane Überwachbarkeit von 0,1 Promille ihrer Teilnehmer technisch zu ermöglichen,

- eine technische Sicherheit im Sinne von Verlässlichkeit der Überwachungseinrichtungen zu garantieren, die zumindest der allgemein zugesicherten Verlässlichkeitsquote ihrer TK-Dienste entspricht.

Die CSP müssen darüber hinaus die Überwachung im Auftrag von ggf. mehreren berechtigten Stellen gleichzeitig durchführen können, ohne dass diese voneinander Kenntnis erlangen können. In der Praxis werden die Daten an das National Technical Assistance Centre übermittelt, dass dazu rund um die Uhr erreichbar ist und auch als

---

75 Gemäß Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002.
76 Vgl. dazu z.B. ETSI TS 101 331 V1.1.1 (2001-08) Technical Specification.

Beratungs- und Informationsbehörde für die Verpflichteten zur Verfügung steht. Das NTAC gibt dann die Daten an die jeweils ermittelnden Stellen getrennt weiter.

6.2.3 Organisatorische Anforderungen

Die CSP sind verpflichtet[77]

- die notwendigen Vorkehrungen für die Überwachung der Telekommunikation innerhalb eines Werktags bereitzustellen,
- ein Audit der Überwachungseinrichtungen zu ermöglichen,
- die Anforderungen der Verordnung so zu erfüllen, dass weder die zu überwachende Person noch unbefugte Dritte von der Überwachung Kenntnis erhalten können.

6.2.4 Ausnahmen

Die Verordnung betrifft nicht

- CSP mit weniger als 10.000 Teilnehmern,
- CSP, deren Aktivitäten sich auf die Gebiete Bankdienstleistungen, Versicherungen, Investment oder andere Finanzdienstleistungen beschränken.

Die Überwachung von bestimmten Personen, wie etwa von Kirchenvertretern, von Journalisten, Rechtsanwälten oder im Gesundheitswesen beschäftigten, ist nur eingeschränkt bzw. unter besonderer vorhergehender Prüfung möglich.

6.2.5 Genehmigungsverfahren für Überwachungsvorkehrungen

Die verpflichteten Unternehmen sollen von der Regierung ein Handbuch erhalten, in dem die technischen und organisatorischen Anforderungen spezifiziert sind. Darin ist u.a. festgelegt, was unter einer Unterstützung, die die Verhältnismäßigkeit wahrt („reasonable assistance“) zu verstehen ist. Ein solches Handbuch liegt derzeit noch nicht vor.

Das Innenministerium erlässt Regelungen für den sicheren und vertraulichen Umgang der berechtigten Stellen mit den bei Überwachungsmaßnahmen erhobenen Daten. Grundsätzlich gilt, dass die Verbreitung, Vervielfältigung und Datenspeicherung auf ein Minimum beschränkt bleiben muss (gemäß des„need-to-know“-Prinzips) (RIPA Sec.

---

77 Gemäß Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002.

15). Werden die Daten nicht mehr für die festgelegten Zwecke benötigt, müssen sie vernichtet werden.

Ein Audit der organisatorischen und technischen Überwachungseinrichtungen eines CSP ist prinzipiell vorgesehen, jedoch noch nicht durch Codes of Practice o.ä. implementiert. Grundvoraussetzung laut RIPA ist, dass die Überwachungsschnittstellen mit den ETSI-Standards konform sein müssen.

6.2.6 Von europäischen Regelungsvorgaben abweichende Regelungen

Das RIPA-Gesetz berücksichtigt nach Angaben der Verantwortlichen ausdrücklich die Anforderungen der Europäischen Menschenrechtskonvention, implementiert im Human Rights Act 1998, insbesondere betreffend den Schutz vor Eingriffen in die Privatsphäre.

Durch RIPA wird außerdem die (jetzt veraltete) Datenschutzrichtlinie der EU (97/66/EC), insbesondere Art. 5 betreffend den Schutz des Fernmeldegeheimnisses, umgesetzt. Eine Umsetzung der kürzlich verabschiedeten Richtlinie 2002/58/EG muss noch erfolgen.

Die im Rahmen von RIPA erlassene Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002 wurde der Europäischen Kommission zur Kenntnis weitergeleitet gemäß der Anforderungen nach Richtlinie 98/34/EC, angenommen durch Richtlinie 98/48/EC.[78]

Anzeichen dafür, dass sich die angestrebten Regelungen im Vereinigten Königreich nicht im Einklang mit den EU-Regularien befinden, können laut Aussagen der Experten nicht ermittelt werden. Entscheidend ist, dass mit RIPA eine gesetzliche Grundlage für Lawful Interception und Data Retention geschaffen wurde, denn das Vorliegen einer gesetzlichen Grundlage ist die Grundvoraussetzung dafür, dass sich die nationalen Regelungen in Übereinstimmung mit den EU-Anforderungen befinden.

Als sehr problematisch wird jedoch das derzeit verfolgte Ziel bewertet, ISP und andere TK-Diensteanbieter auf Basis einer freiwilligen Vereinbarung zur Herausgabe von Verkehrsdaten oder Kundendaten indirekt zu verpflichten. Dies wird im Rahmen des RIPA Part I Chapter II und des Anti-Terrorismusgesetzes diskutiert. Die Vorteile einer freiwilligen Regelung werden von Seiten der Regierung darin gesehen, dass dabei die Kosten von den Unternehmen getragen würden. Rechtsexperten sind jedoch der Auffassung,

---

78 Vgl. Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations sowie Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations. Beide Richtlinien haben die Interoperabilität von technischen Systemen zum Ziel.

dass eine solche freiwillige Übereinkunft nicht in Übereinstimmung mit den EU-Bestimmungen steht, da diese ausdrücklich eine gesetzliche Grundlage fordern.

6.3 Voraussetzungen für die Überwachung

6.3.1 Fälle, in denen das Überwachen der TK angeordnet werden kann

Nach RIPA ist die Überwachung der individuellen Kommunikation zu folgenden Zwecken zulässig (RIPA Sec. 5 (3)):

- im Interesse der nationalen Sicherheit,
- zum Schutz vor bzw. zur Aufdeckung von schweren Straftaten,
- im Interesse des wirtschaftlichen Wohlergehens des Vereinigten Königreichs,
- für jeden weiteren Fall, der den o.g. Zwecken entspricht, wenn die Überwachung vom zuständigen Minister angeordnet wird.

Data Retention

Die Kommunikationsdatengewinnung gemäß RIPA Part I Chapter II ist zu weiter reichenden Zwecken zu ermöglichen, nämlich:

- 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 Anti-Terrorismus-Gesetz von 2001 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.

Darüber hinaus ist es den Unternehmen gestattet, Daten für die Erbringung ihrer Geschäftstätigkeit, für die Rechnungstellung oder aus Gründen der Netzwerksicherheit zu speichern.

6.3.2 Genehmigung einer Überwachungsmaßnahme

Eine Anordnung für die Überwachung der individuellen Kommunikation einer Person nach RIPA wird durch den Innenminister (Home Secretary) bzw. durch sein schottisches Pendant (Scottish Executive) unterzeichnet[79] und nur in Ausnahmefällen von einem Vertreter.[80] Änderungen der Anordnung können durch dazu autorisierte hohe Beamte des Home Office erfolgen, sind diese Änderungen äußerst dringend auch von einem dritten Kreis von Personen mit niedrigerem Rang (Director General, Deputy Director General, Service Legal Adviser).

Die Unterzeichnung durch den Minister erfolgt auf Antrag eines der folgenden Leitungspersönlichkeiten der Polizei- und Strafverfolgungsbehörden bzw. in ihrem Namen:

- des Director-General of the Security Service,
- des Chief of the Secret Intelligence Service,
- des Director of Government Communications Headquarters,
- des Director General of the National Criminal Intelligence Service,
- des Commisioner of Police of the Metropolis,
- des Chief Constable of the Royal Ulster Constabulary,
- eines Chief Constable einer Einheit der schottischen Polizei,
- der Commissioners of Customs and Excise,
- des Chief of Defence Intelligence,
- Personen, die auf Grund internationaler gegenseitiger Abkommen dazu berechtigt sind.

---

79 Prinzipiell ist nach dem Gesetz dies jedem Minister möglich; Konvention ist, dass die genannten Minister die Anordnung vornehmen.

80 Strategische Überwachungen in Zusammenhang mit Kommunikation im Ausland werden vom Außenminister genehmigt.

Besondere Relevanz hat die Begründung für die Beantragung einer Überwachung. Die Maßnahme muss als verhältnismäßig und notwendig eingestuft werden können. Das kann beispielsweise bedeuten, dass die Informationen nicht auf eine andere Weise gewonnen werden können. Außerdem dürfen die damit verbundenen Anforderungen an den Kreis der verpflichteten CSP nicht unverhältnismäßig sein, d.h. z.B. nicht zu hohen technischen und organisatorischen Aufwand und damit zu hohe Kosten beinhalten.

Ausnahme: Überwachung ohne Anordnung

Eine Überwachung, ohne dass eine Anordnung unterzeichnet wurde, ist zulässig, wenn sie mit Einwilligung eines der Kommunikationspartner erfolgt. Von Unternehmen gespeicherte Kommunikationsdaten können ohne Anordnung herausgegeben werden[81] (RIPA Sec. 1 (5)).

Darüber hinaus darf ein CSP Überwachungsmaßnahmen in seinem Netz durchführen, wenn dies für technische Zwecke erforderlich ist.

Es ist außerdem Unternehmen und auch öffentlichen Behörden gestattet, Kommunikation zu überwachen, wenn dies dazu erforderlich ist, um die Arbeitsweise ihrer Angestellten zu überwachen („Lawful Business Practice").[82] Dazu ist es einem Arbeitgeber beispielsweise erlaubt, Mitschnitte von Telefongesprächen anzufertigen oder E-Mail-Kommunikation zu speichern. Er muss die Mitarbeiter aber über diese Praxis informieren.

Data Retention

Der Zugriff auf bei den CSP vorhandene oder durch diese zu gewinnende Daten gemäß RIPA wird nicht durch eine Anordnung des Ministers, sondern durch eine sog. Autorisierung von definierten hohen Beamten der Strafverfolgungsbehörden ermöglicht.

6.3.3 Möglicher Zeitraum der Überwachung

Anordnungen nach RIPA erstrecken sich auf einen Zeitraum von bis zu drei Monaten und können dann in Intervallen von drei Monaten (bei schweren Straftaten) und sechs Monaten (bei Gefährdung der nationalen Sicherheit und des wirtschaftlichen Wohlergehens) verlängert werden.

---

81 Vergleichbar mit einer Beschlagnahmung von Daten.

82 Die Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 („LBP Regulations") können unter der Homepage des Department of Trade and Industry www.dti.gov.uk/cii/regulation.html eingesehen werden.

Dringende Anordnungen, die nicht vom Innenminister persönlich unterzeichnet sein müssen, gelten nur für fünf Werktage, wenn sie nicht durch eine Anordnung des Ministers ersetzt werden.

6.3.4 Überprüfung der Rechtmäßigkeit der Maßnahme durch die Verpflichteten

Es konnten keine derartigen Verpflichtungen aus den Dokumenten und Expertengesprächen eruiert werden.

Bei der ehemaligen Royal Mail – jetzt Consiglia – ist es jedoch nach Kenntnis von Experten üblich, Anträge auf Überwachung zu prüfen. Dies liegt darin begründet, dass mehrfach Privatdetektive versucht haben, unter dem Vorwand polizeilicher Ermittlungen an Informationen zu gelangen. Es erscheint nicht ausgeschlossen, dass auch Unternehmen solche Kontrollen zu ihrer eigenen Absicherung vornehmen, um sich nicht dem Vorwurf eines Verstoßes gegen die TK-Datenschutzbestimmungen aussetzen zu müssen.

6.4 Durchführung der Überwachung

6.4.1 Erforderliche Angaben

Überwacht werden Personen, die in der Anordnung des Innenministeriums genannt werden. Die Überwachung wird spezifiziert durch die angegebenen Telekommunikationsadressen (Telefonnummern, E-Mail-Adressen etc.). Ändern sich die Telekommunikationsanschlüsse, ist eine Modifikation der Anordnung erforderlich, nicht jedoch eine neue Anordnung.

Die berechtigten Stellen geben folgende Angaben an die CSP weiter:

- Kopie der vom Innenminister (oder in dringenden Fällen seines Vertreters) unterzeichneten Anordnung,
- die für die Überwachung notwendigen Nummern, Adressen und sonstigen Kennungen,
- Name der Person, die in dringenden Fällen die Anordnung modifizieren darf,

- weitere Informationen der berechtigten Stelle, die weitere Details für die Überwachung und die Weiterleitung der überwachten Daten enthalten können sowie Kontaktadressen der berechtigten Stelle. Die berechtigten Stellen können für diese Zwecke Handbücher erarbeiten. Solche liegen noch nicht vor.

Es werden nur die den jeweiligen CSP betreffenden Angaben weitergegeben.

6.4.2 Art der zu überwachenden Telekommunikation

Zu Überwachen ist Telekommunikation während des Übertragungsprozesses sowie auch dann, wenn die Telekommunikation, um übertragen werden zu können, im Telekommunikationssystem vorübergehend gespeichert wird. Eine Anordnung kann demzufolge sowohl Kommunikation im Zustand der Übertragung als auch im Zustand der Speicherung betreffen.[83] Die Forderung nach Überwachbarkeit der Telekommunikation erstreckt sich auf jegliche Art der Telekommunikation und ist damit unabhängig von einer bestimmten technischen Ausgestaltung.

6.4.3 Übermittlung an die berechtigten Stellen

Die zu überwachende Telekommunikation wird an einen von der berechtigten Behörde definierten Übergabepunkt weitergeleitet, d.h. in der Praxis, die Daten werden zunächst an die NTAC übermittelt, die diese dann an die Behörden weiterleitet. Überwachungsmaßnahmen verschiedener Behörden, die die gleiche Person betreffen, müssen so durchgeführt werden, dass die jeweiligen Behörden nicht von den weiteren Maßnahmen Kenntnis erlangen können. Dazu werden die Daten getrennt an die NTAC übermittelt und von dort auch getrennt weitergeleitet.[84]

6.4.4 Unterschiedliche technische Einrichtungen für verschiedene Überwachungsanforderungen

Die konkreten Anforderungen, die das Innenministerium in seinen Mitteilungen („Notices“) gemäß RIPA an die CSP stellt, liegen noch nicht vor. Sie werden voraussichtlich nicht öffentlich. Es wird von Experten vermutet, dass für strategische Überwachungsmaßnahmen andere Anforderungen gestellt werden. Es ist jedoch davon auszugehen, dass diese auch in Zukunft nicht öffentlich gemacht werden.

---

83 Diese Spezifizierung scheint vor allem notwendig im Hinblick auf die Überwachung von E-Mail-Kommunikation (vgl. dazu Home Office (Hrsg.) (2002): Interception of Communications. Code of Practice. Pursuant to Section 71 of the Regulation of Investigatory Powers Act 2000).

84 Die Industrie schlägt vor, zur Kostenersparnis die Daten gesammelt an die NTAC zu übertragen und die Trennung nach verschiedenen Überwachungsmaßnahmen erst dort vorzunehmen. Der Vorschlag wurde bisher abgelehnt.

Data Retention

Die Herausgabe von gespeicherten Daten an die Strafverfolgungsbehörden erfolgt zur Zeit nach einer informellen Praxis, die auf einer Regelung in der Datenschutzgesetzgebung (Data Protection Act 1998 Sec. 29) des Vereinigten Königreichs beruht. Wie ein Experte erläuterte, ist danach die Herausgabe von Daten möglich, wenn ein sog. „Data Controller" (d.h. jemand, der im Rahmen seiner Geschäftstätigkeit Zugang zu den benötigten Daten hat), also beispielsweise ein CSP, die Strafverfolgungsbehörden in einem konkreten Fall unterstützt. Voraussetzung dafür ist erstens, dass der CSP die Daten ohnehin gespeichert hat bzw. während seiner Geschäftsprozesse gewinnt, dass er zweitens davon Kenntnis hat, dass diese Daten zum Zweck der Strafverfolgung relevant sind und drittens die Strafverfolgungsbehörden keine andere Möglichkeit besitzen, eine Straftat aufzudecken.

In der Praxis setzen die Strafverfolgungsbehörden die CSP von ihrem Verdacht gegen eine Person in Kenntnis und begründen, warum sie die Herausgabe von Daten für verhältnismäßig und notwendig halten. Dadurch wird der CSP indirekt in die Lage versetzt, die Daten herausgeben zu können, da er nun von der strafrechtlichen Relevanz Kenntnis erlangt hat. Datenschützer kritisieren diese Praxis als rechtlich unzureichend und geben zu bedenken, dass sie vermutlich vor Gericht – auch auf europäischer Ebene - nicht standhalten würde. Eine gesetzliche Regelung wird deshalb für unabdingbar gehalten, um diese geübte Praxis zu beenden.

6.4.5 Echtzeit-Überwachung oder Speicherung

Nach RIPA muss eine Übertragung der zu überwachenden Telekommunikation in Echtzeit erfolgen. Dies ist in der entsprechenden Verordnung noch einmal ausdrücklich festgelegt. Daten, die zum Zweck der Übertragbarkeit zwischengespeichert werden müssen, können jedoch ebenfalls überwacht werden.[85]

Der noch nicht in Kraft getretene Teil des RIPA Part I Chapter II sieht vor, dass eine Autorisierung zur Weitergabe der beim Diensteanbieter vorhandenen bzw. zu gewinnenden Daten nur einen Zeitraum von nicht länger als einem Monat betrifft (RIPA Sec. 23 (4)). Die Autorisierung kann verlängert werden.

Grundsätzlich ist eine Speicherung von Daten durch den Anti-terrorism Crime and Security Act 2001 gestattet.[86] Die Dauer richtet sich dabei nach der Art der Daten und liegt zwischen mindestens 6 bis hin zu 12 Monaten.

---

85 Dies ist z.B. für die Überwachung von E-Mail-Kommunikation relevant.
86 Vgl. General Secretariat of the Council (2002).

Von den Strafverfolgungsbehörden wurden Speicherzeiträume von bis zu sieben Jahren gefordert. Diese Zeitspanne haben der Datenschutzbeauftragte sowie die Industrie scharf kritisiert. Die Diskussion um die praktische Ausgestaltung von Data Retention und die Ausarbeitung von Codes of Practice in diesem Bereich wird voraussichtlich noch einige Zeit in Anspruch nehmen, so dass heute noch keine definitiven Aussagen zum Umgang mit Speicherfristen getroffen werden können.

6.5 Kontroll- und Sanktionsmaßnahmen

6.5.1 Kontrollinstanzen

Zu den durch das RIPA installierten Kontrollinstanzen gehören

- Interception of Communications Commissioner: Der unabhängige Beauftragte verfasst einen jährlichen Bericht an den Premierminister. Dieser entscheidet über die Veröffentlichung.
- Investigatory Powers Tribunal: Das von der Regierung unabhängige Gericht ist zuständig für Beschwerden, die Abhörmaßnahmen betreffen. Es wurde mit dem RIPA etabliert und löst das vormalige Interception of Communications Tribunal unter dem vorhergehenden Gesetz ab.

Überwachungskompetenzen der Geheimdienste werden von der Institution des Surveillance Commissioner kontrolliert. Beschwerden in diesem Zusammenhang können ebenfalls an das o.g. Gericht ergehen.

6.5.2 Berichtspflichten

Alle in die Überwachungsmaßnahmen laut RIPA involvierten Behörden und Unternehmen sind verpflichtet, den Interception of Communications Commissioner bei seiner Arbeit zu unterstützen und Information für den jährlichen Bericht beizubringen.

Insbesondere haben die berechtigten Stellen für diese Zwecke Kopien der Anordnungen, der Anträge auf Anordnung sowie die erfolgten Modifikationen aufzubewahren. Sie müssen ebenfalls die Dokumente archivieren, die die Gründe für die Ablehnung von Anträgen auf Überwachungsanordnungen enthalten.

6.5.3 Statistiken

Von den berechtigten Stellen ist eine Statistik über Beginn und Ende der Überwachungsmaßnahmen zu führen. In den Berichten des Interception of Communications Commissioner sind die durchgeführten Abhörmaßnahmen summarisch aufgeführt (vgl. Tabelle 6-1). Seit Verabschiedung des RIPA wird in der Statistik nicht mehr zwischen den Maßnahmen, welche die Telekommunikation und denjenigen, die die Post betreffen, unterschieden. Nach Meinung des Interception of Communications Commissioner sollen die Überwachungsstatistiken, die Nordirland betreffen, aus Sicherheitsgründen nicht veröffentlicht werden. Das Innenministerium ist seit Bestehen der jährlichen Überwachungsberichte dieser Auffassung gefolgt. Nach Einschätzung von Experten werden im Durchschnitt bis zu 500 Maßnahmen gleichzeitig durchgeführt.[87]

Tabelle 6-1: Anzahl der Überwachungsmaßnahmen im Vereinigten Königreich (1993 - 2001) (außer Nordirland)

Jahr	Gesamtzahl der Anordnungen
1993	1.005
1994	961
1995	1.047
1996	1.301
1997	1.647
1998	1.913
1999	1.933
2000 (bis Sept.)*	1.662
2000 (Okt.-Dez.)**	661
2001	1.445

Quelle: Annual Report of the Interception of Communications Commissioner for 1999 (berücksichtigt sind Maßnahmen im Bereich Telekommunikation von 1993 - 1999, die im Verlauf des genannten Jahres angeordnet wurden), Report of the Interception of Communications Commisioner for 2000; Report of the Interception of Communications Commisioner for 2001; * nach dem Interception of Communications Act 1985 (nur Telekommunikation, ohne Post); ** nach RIPA (in der Statistik nach RIPA werden Post und Telekommunikation zusammengefasst, die Anordnungen sind auf Personen bezogen)

87 Zum Vergleich: In UK leben 59,7 Mio. Menschen.

6.5.4 Sanktionen

Der Interception of Communications Commisioner stellt für das Berichtsjahr 2001 insgesamt 43 Fehler in der Anwendung des RIPA fest. Alle Verstöße sind nach Auffassung des Beauftragten auf Irrtümer und Missverständnisse zurückzuführen. Absichtliche Verstöße konnten nicht festgestellt werden. Es handelt sich z.B. um Überschreitungen von Zeitvorgaben bei der Beantragung von Anordnungen, Verwechselungen der Postleitzahl oder falsch angegebenen Telefonnummern. Beispiele sind in dem öffentlichen Bericht des Beauftragten enthalten, der vertrauliche Bericht enthält eine ausführliche Liste aller aufgetretenen Probleme.

Hält ein CSP die an ihn gestellten Anforderungen für unverhältnismäßig und weigert er sich, diesen nachzukommen, drohen Sanktionen.

Eskaliert etwa ein Konflikt in der Art, dass sich das Unternehmen nicht in der Lage sieht, bestimmte Verpflichtungen zu erfüllen, liegt es in der Kompetenz des Innenministers, weitere rechtliche Schritte einzuleiten. Werden beispielsweise die technisch-administrativen Anforderungen nicht erfüllt, sind Freiheitsstrafen von bis zu zwei Jahren denkbar; werden Geheimhaltungsvorschriften von Seiten der CSP nicht eingehalten, Strafen von bis zu fünf Jahren.

Seit Bestehen des Investigatory Powers Tribunal im Oktober 2000 gingen bis Ende 2001 102 Beschwerden ein. Bisher konnte das Gericht in den 71 untersuchten Fällen keine Zuwiderhandlungen gegen RIPA oder den Human Rights Act 1998 feststellen, so dass noch keine Sanktionen aufgrund von Urteilen dieses Gerichts notwendig geworden sind.

6.6 Kosten

6.6.1 Bewertung des Aufwands durch die Verpflichteten

Wie auch in Deutschland werden die Kosten für die Sicherstellung der Überwachbarkeit der Telekommunikation von den TK-Anbietern und Betreibern von TK-Anlagen als erheblich eingestuft. Besonders die ISP, die durch die neue Gesetzgebung erstmals verpflichtet sind, technische und administrative Vorkehrungen zu treffen und im Rahmen von Data-Retention-Regelungen wahrscheinlich umfassende Speichereinrichtungen installieren müssen, protestieren gegen die Anforderungen der Regierung. Die zentrale Frage, die zurzeit in UK erörtert wird, lautet, ob RIPA ein Risiko für die weitere Geschäftstätigkeit von CSP darstellt. Industrie-Organisationen wie ICAF widmen sich der Beratung und der Lobbytätigkeit auf diesem Gebiet und sehen momentan aufgrund fehlender Spezifizierungen (Handbücher, Codes of Practice etc.) keine eindeutige Antwort auf diese Frage. Sie schätzen die möglichen finanziellen Auswirkungen jedoch als erheblich ein.

Die geplante freiwillige Übereinkunft zu Dauer und Art der Speicherung von Daten ist noch nicht zustande gekommen. Offizielle Erklärungen liegen dazu nicht vor. Aus der Presse[88] ist zu entnehmen, dass die ISP, vertreten von der Internet Services Providers' Association (ISPA), dem Innenministerium in einem Brief im Oktober 2002 mitgeteilt haben, dass sie eine längere Speicherung der Daten als bisher für nicht gesetzeskonform halten. Datenschützer bezeichnen dies bereits als endgültiges Scheitern einer freiwilligen Lösung und erwarten eine Verpflichtung der ISP durch Verordnung oder eine Gesetzesnovelle.

6.6.2 Kostenübernahme und Aufwandsentschädigungen

Das Innenministerium ist durch RIPA (Sec. 14) verpflichtet, für eine finanzielle Entschädigung zu sorgen. Die Regierung hat für die Zahlungen rund 20 Mio. Pfund für den Zeitraum von 2001 bis 2004 eingestellt.[89]

Die Kosten für die Durchführung von Überwachungsmaßnahmen sollen annähernd gedeckt werden. Es ist noch nicht präzisiert, welche Kosten in die Berechnung einfließen dürfen (Hardware, Software, Personalkosten, etc.). Um zu vermeiden, dass CSP Gewinne durch die Durchführung von Überwachungsmaßnahmen erzielen könnten, existieren keine festen Preislisten in Bezug auf die Aufwendungen. Im Bereich der Sprachtelefonie ist die Zahlung von Aufwandsentschädigungen eine seit langem geübte Praxis, ohne dass dazu genauere, veröffentlichte Regelungen vorlägen.

---

88 Vgl. The Guardian v. 22.10.2002 „Internet providers say no to Blunkett".
89 Vgl. Shaw Pittman Alert, December 2000, No. 5 (www.shawpittman.com).

7 Rahmenbedingungen für Lawful Interception in den USA

In den USA bestehen seit Anfang der 90er Jahre detaillierte Regelungen über die Verpflichtungen von Netzbetreibern hinsichtlich der Sicherstellung von TK-Überwachbarkeit. Obwohl die Anforderungen der Strafverfolgungsbehörden mit der Zusicherung von Kostenerstattungen einhergehen, hat sich die flächendeckende Implementierung von gesetzeskonformer Technologie als problematisch herausgestellt. Zahlreiche Unternehmen haben von der Möglichkeit Gebrauch gemacht, eine Verlängerung der Fristen zu beantragen, so dass heute, beinahe zehn Jahre nach Verabschiedung der entsprechenden gesetzlichen Regelungen, noch keine umfassende TK-Überwachbarkeit auf der Basis permanent vorhandener technischer Einrichtungen erreicht ist.

7.1 Rechtliche Grundlagen

7.1.1 Grundlagen in der TK-Gesetzgebung

Die TK-Überwachung ist in den USA im Rahmen der Strafgesetzgebung geregelt. Die TK-Gesetze enthalten keine Regelungen dazu. Die Regulierungsbehörde Federal Communications Commission (FCC) ist jedoch mit der Umsetzung der technischen und organisatorischen Überwachungsanforderungen an die TK-Anbieter und -Anlagenbetreiber befasst und hat dazu im Rahmen des Communications Assistance for Law Enforcement Act von 1994 (CALEA) Verordnungen erlassen. Sie ist außerdem in den aktuellen Diskussionsprozess um Form und Zeitrahmen des Umsetzungsprozesses involviert.

7.1.2 Einschlägige Rechtsvorschriften

Auf Basis der folgenden Gesetzestexte ist die Überwachung der Telekommunikation zum Zweck der Strafverfolgung im Rahmen des US-amerikanischen Criminal Code (Strafgesetz) möglich:[90]

- Omnibus Crime Control and Safe Streets Act von 1968 (OCCSSA),[91]
- Electronic Communications Privacy Act von 1986 (ECPA).[92]

---

90 Die rechtlichen Grundlagen sind umfassend dargestellt in DoJ (2002).

91 18 U.S.C. 2510-2522 (genannt „Title III“). Das Gesetz legt grundsätzlich die Kompetenz des Staates fest, auf gesetzlicher Basis TK-Überwachungen vorzunehmen.

Ersteres Gesetz legt in „Title III“, dem „Wiretap Statute“, fest, dass alle TK-Anbieter und -Anlagenbetreiber verpflichtet sind, alles zu tun, um die Strafverfolgungsbehörden bei der Überwachung von Kommunikationsinhalten zu unterstützten. Letzteres erweitert die Befugnisse der Strafverfolgungsbehörden hinsichtlich der Überwachung neuer elektronischer Kommunikationstechnologien und regelt die Möglichkeit der Beschlagnahmung von Daten.

Des weiteren ist die Überwachung von Kommunikationsdaten mittels sog. Pen Register oder Trap and Trace Devices laut Criminal Code möglich. Dieses „Pen/Trap Statute“ ist insbesondere relevant für die Überwachung von Internet-Kommunikation.

Der im Jahr 2001 nach den Anschlägen des 11. September verabschiedete

- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act 2001 (kurz „USA Patriot Act“ genannt)

ist insofern für die TK-Überwachung von Bedeutung, als er zwar nicht die Maßnahmen als solche definiert, jedoch die Liste der Anlässe für die Rechtmäßigkeit einer Überwachung erweitert und zwar sowohl für „Wiretaps“ und „Roving Wiretaps“ als auch für „Pen registers“ und „Trap and Trace Devices“.[93] Bemerkenswert im Zusammenhang mit diesem Anti-Terrorismus-Gesetz ist, dass es keine neuen, zusätzlichen Anforderungen an die TK-Anbieter und –Anlagenbetreiber bezüglich der Bereithaltung von technischen und organisatorischen TK-Überwachungsvorkehrungen enthält.

Somit bleibt weiterhin der Communications Assistance for Law Enforcement Act von 1994 (CALEA)[94] maßgeblich. CALEA legt die Pflichten der TK-Netzbetreiber („telecommunication´s carrier“, CALEA Präambel) hinsichtlich der Kooperationspflichten bei Lawful Interception fest und fordert auch von den Herstellern von TK-Ausrüstungen die Entwicklung von CALEA-konformer Hard- und Software. Die FCC hat im Rahmen der Entwicklung eines Interim-Standards eine Verordnung mit weiteren Anforderungen erlassen, die die Pflichten der Netzbetreiber sowie der TK-Equipment-Hersteller spezifiziert (sog. „Punch List“). Seitdem hält die Diskussion um die Umsetzbarkeit der Forderungen an. CALEA wird von manchen Experten als Misserfolg beurteilt[95] und zwar nicht zuletzt deshalb, weil es bisher nicht gelungen ist, für eine flächendeckende Verfügbarkeit von Überwachungstechnik zu sorgen. Der Implementationsprozess gestaltet sich sehr komplex und aufwändig (vgl. Tabelle 7-1).

Der Stichtag, bis zu dem die Netzbetreiber die CALEA-Anforderungen umgesetzt haben sollten, war der 25. Oktober 1998, aber die FCC hat schon frühzeitig diesen Termin auf

---

92 18 U.S.C. 2701. Das Gesetz über Datenschutz in der elektronischen Kommunikation erweitert die gesetzlichen Überwachungsbefugnisse des Staates nach „Title III“ auf die neuen elektronischen Kommunikationstechnologien.
93 Vgl. dazu ausführlich Pallasky, A. (2002).
94 47 U.S.C. 1001-1010
95 So die Einschätzung von Elder, vgl. Elder, D. (2002).

den 30. Juni 2000 verschoben. Für eine große Anzahl von Unternehmen wurde ein weiterer pauschaler Aufschub bis zum 30. Juni 2002 gewährt. Da sich abzeichnete, dass die Mehrzahl auch diese Frist nicht einhalten konnte, war es möglich, mit der Begründung, die Anforderungen seien derzeit nicht mit vertretbarem Aufwand zu realisieren, bei der FCC einen Antrag auf weiteren Aufschub zu stellen. Somit ist mehr als vier Jahre nach der Veröffentlichung der „Punch List“ die flächendeckende Verfügbarkeit von Überwachungstechnik in den TK-Netzen noch nicht gewährleistet.[96]

96 Vgl. Elder, D. (2002), S. 15. Die Fortschritte sind darüber hinaus in den Berichten des FBI und des Justizministeriums an den Kongress dokumentiert, vgl. aktuell FBI / DoJ (2001).

Tabelle 7-1: CALEA im Überblick: Fortschritte bei der Implementierung

Section		CIS	Industry	FCC	Other
Definitions	102	• Provided input to the FCC	• Provided input to the FCC	• **Second Report & Order**- Definition of a telecommunications carrier	
Notices of Capacity Requirements	104	• **Final Notice of Capacity** for local exchange services, cellular and broadband PCS • Notice of Inquiry and **Further Notice of Inquiry** for other technologies	• Provided input the CIS • Submitted carrier statements • Challenged Final Notice of Capacity in Court		• Industry associations challenged the Final Notice of Capacity in Court
Systems Security and Integrity (SS&I)	105	• Provided input to the FCC	• Provided input to the FCC	• **Memorandum Opinion and Order** outlining carriers´SS&I responsibilities	
Cooperation of Equipment Manufacturers and Providers of Telecommunications Support Services	106	• Consulted with individual manufacturers and providers of support services in their development of solution(s)	• Solution developed by switch manufacturers and peripheral equipment providers		
Technical Requirements and Standards; Extension of Compliance Date	107	• Consulted with the industry in the development of J-STD-025 • Filed deficiency petition with FCC • Provided input to the FCC • Adopted **Flexible Deployment** Initiative	• **J-STD-025** for local exchange, cellular and broadband PCS • Requested extension of 10/25/98 compliance date	• **Third Report & Order** determining required capabilities • Granted extension of 10/25/98 date until 6/30/00	• Privacy Groups filed petition of deficiency with FCC
Payment of Costs of Telecommunications Carriers to Comply with Capability Requirements	109	• **Cost Recovery Regulations** with definition of "installed or deployed" • Reimbursed industry for a number of technical solutions	• Provided input to the CIS • Challenged Cost Recovery Rules in Court		• Industry associations challenged the Final Notice of Capacity in Court
Authorization of Appropriations	110				• To date, Congress has appropriated USD 499 million
Reports	112	• Submitted six **Annual Reports to Congress**			

Quelle: DoJ / FBI

7.1.3 TK-Dienste, für die die Überwachbarkeit gewährleistet sein muss

Grundsätzlich wird in der einschlägigen „Wiretap"-Gesetzgebung[97] festgelegt, dass folgende Kommunikation unter Beachtung der gesetzlichen Bestimmungen überwacht werden darf:

- „oral communication", d.h. persönliche, mündliche Kommunikation (für TK-Überwachung nicht relevant),
- „wire communications", d.h. elektronische Kommunikation, die menschliche Sprache beinhaltet. Dazu ist es für die Definition ausreichend, wenn die Kommunikation irgendwo, also z.B. bei Satelliten- oder Mobiltelefonie, über ein Kabel geführt wird, und sei es auch nur in einer Vermittlungsstelle,
- „electronic communication", d.h. alle übrigen Arten von elektronischer Kommunikation, mit Ausnahme von z.B. finanzielle Transaktionen,

Letztere Kategorie wurde durch den ECPA im Jahr 1986 eingeführt, um Kommunikation über Pager, Faxgeräte und computergestützte Datenübertragung sowie auch Internet-Kommunikation zu berücksichtigen.

Die potenziellen „Wiretap"-Überwachungsmethoden für Telekommunikation umfassen insgesamt:

- Überwachung von „phone wire communication" (alle Arten von Telefonie: drahtgebunden und drahtlos), (83 Prozent der Überwachungsmaßnahmen, davon die Mehrzahl drahtlose Telefonie),[98]
- „electronic wiretap" (Pager, Faxgeräte, E-Mail und andere Datenübertragung) (6 Prozent der Überwachungsmaßnahmen),
- Kombination von Methoden (4 Prozent der Überwachungsmaßnahmen).

Darüber hinaus werden in diesem Gesetz auch Lauschaktionen (Abhören mittels Mikrofon) geregelt, die jedoch vollständig außerhalb des hier betrachteten Rahmens der Überwachung der Telekommunikation fallen.

Besonderheit

Der EPCA legt u.a. fest, dass ein spezifischer Ort für die Implementation des Überwachungsmediums nicht mehr angegeben werden muss, wenn begründet werden kann,

---

97 18 U.S.C. 2519(1), Omnibus Crime Control and Safe Streets Act von 1968. Ausführliche Erläuterungen unter DoJ (2002), Kapitel D.

98 Zahlen zur Durchführung von Überwachungsmaßnahmen beziehen sich jeweils auf den aktuellen Report der AO von 2002 (falls nicht anders angegeben).

dass eine solche Spezifizierung keinen Sinn macht, da es darum geht, eine bestimmte Person und nicht einen bestimmten Telefonanschluss oder Raum zu überwachen.[99] In diesen Fällen können „Roving Wiretaps“, d.h. mobile Überwachungen, eingesetzt werden. Der Intelligence Authorization Act von 1999 ergänzt diese Bestimmung mit derselben Intention.

7.1.4 Zweck der Überwachung

Nach dem Omnibus Crime Control and Safe Streets Act von 1968 ist das Abhören von Telekommunikation grundsätzlich verboten. Eine Ausnahme bildet die gesetzlich gestattete TK-Überwachung – „Wiretaps“ und „Pen/Trap and Trace“ - für Zwecke der Strafverfolgung sowie die Beschlagnahmung von Daten nach ECPA.

7.1.5 Unterschiede zwischen individuellen Überwachungsmaßnahmen der Strafverfolgungsbehörden und denen der Sicherheitsbehörden

Die strategische TK-Überwachung ist im Foreign Intelligence Surveillance Act (FISA) von 1978[100] geregelt. Es existieren zum Teil eigene Überwachungseinrichtungen sowie Kontrollmaßnahmen für diese personenbezogenen TK-Überwachungen, die der Prävention dienen.

Im Jahr 2000 wurde bekannt, dass das FBI im Rahmen von FISA ein Überwachungssystem namens Carnivore (heute genannt DSC 1000 Programm) entwickelt hat, das bei einem ISP fallweise installiert werden kann und mittels dessen die Telekommunikation, die einer bestimmten Person auf Grund einer eindeutigen Kennung zuzuordnen ist, aus dem gesamten Verkehr eines paketvermittelnden Netzes, insbesondere E-Mail und Webtraffic, der über die Einwählknoten dieses ISP läuft, ausgefiltert und der überwachenden Stelle zugänglich gemacht werden kann. Das System wird weiterhin eingesetzt, obwohl eine vom Justizministerium veranlasste Untersuchung Änderungen Ende Dezember 2000 angemahnt hat.[101] DCS 1000 dient z.B. der Durchführung von „Pen/Trap and Trace“, wenn der ISP keine eigene entsprechende technische Ausrüstung zur Verfügung hat oder zur Verfügung stellen will.[102]

---

99 18 U.S.C. 2518 (11)
100 50 U.S.C. 1801
101 Vgl. Testimony of Robert Corn-Revere, before the Subcommittee on the Constitution of the Committee on the Judicary, United States House of Representatives, The Fourth Amendment and the Internet, April 6, 2000, abrufbar unter www. house.gov/judicary/corn0406.htm, zit. nach EPIC/PI (Eds.) (2002), S. 390.
102 Vgl. dazu ausführlich DoJ (2002), Kapitel C.

7.2 Verpflichtungen für die TK-Anbieter und Betreiber von TK-Anlagen

7.2.1 Kreis der Verpflichteten

Alle TK-Anbieter und –Anlagenbetreiber, also alle Netzbetreiber und Service Provider, sind verpflichtet, die berechtigten Stellen bei der Durchführung von TK-Überwachungsmaßnahmen – „Wiretaps“ und „Pen/Trap and Trace“ - zu unterstützen.

Im Criminal Code heißt es dazu:

„An order authorizing the interception of a wire, oral, or electronic communication under this chapter shall, upon request of the applicant, direct that **a provider of wire or electronic communication service, landlord, custodian or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference** with the services that such service provider, landlord, custodian, or person is according the person whose communications are to be intercepted.“[103] [Hervorhebung nicht im Original].

Dazu müssen die Netzbetreiber technische Einrichtungen permanent zur Verfügung stellen mit einer ständigen Verfügbarkeit von Personal („7x24“), ISP ohne eigenes Netz nur fallweise.[104]

Die speziellen Verpflichtungen für Netzbetreiber (Carrier) sind in CALEA 47 U.S.C. 1002 spezifiziert. Betroffen sind alle Unternehmen, die die Übertragung von „wire“ oder „electronic communications“ für die Öffentlichkeit geschäftsmäßig anbieten. Netzbetreiber umfassen alle TK-Anbieter und –Anlagenbetreiber außer denjenigen ISP, die als „Information Service Provider“ am Markt agieren und kein eigenes Netz betreiben. Bei CALEA handelt es sich aber ausdrücklich um eine technikneutrale Regelung, d.h. die Art der Übertragung (z.B. paketorientiert oder anderweitig) hat keinen Einfluss darauf, ob ein Unternehmen unter die CALEA-Verpflichtungen fällt oder nicht.

CALEA enthält auch eine Vorschrift für die Hersteller von Sprachtelefonie-Technologie, Überwachungslösungen in ihre Produkte zu integrieren (47 U.S.C. 1005).

Die Verpflichtungen gemäß CALEA wurden in einer Debatte im Kongress folgendermaßen spezifiziert:[105]

---

103 18 U.S.C. 2518(4).

104 Die Verpflichtung ergibt sich im Wesentlichen aus einer Grundsatzentscheidung des Supreme Courts aus dem Jahr 1977 (United States v. New York Telephone Co., No. 76-835, Supreme Court of the United States, 434 U.S. 159; 98 S. Ct. 364; 54 L. Ed. 2d 376; 1977 U.S. LEXIS 161, Argued October 3, 1977, December 7, 1977).

105 Vgl. H. Rep. No. 103-827, 103d Cong., 2d Sess. 9 (1994), zit. nach DoJ / FBI (2001), S. 3.

„(1) isolate expeditiously the content of targeted communications transmitted by the carrier within the carrier's service area; (2) isolate expeditiously information identifying the origin and destination of targeted communications; (3) provide intercepted communications and call identifying information to law enforcement so they can be transmitted over lines or facilities leased by law enforcement to a location away from the carrier's premises; and (4) carry out intercepts unobtrusively, so targets are not made aware of the interception, and in a manner that does not compromise the privacy and security of other communications."

Die Verantwortlichkeit für die Implementierung von CALEA hat das Justizministerium an das FBI delegiert. Innerhalb der FBI Laboratory Division wurde die Abteilung CIS – CALEA Implementation Section gegründet. CIS versteht sich als Interessenvertreter der Strafverfolgungsbehörden und vertritt diese vor dem Kongress, in Diskussionen mit der FCC und anderen Regierungsbehörden sowie der TK-Industrie.[106] Zur Gestaltung der technischen Anforderungen hat CIS das Law Enforcement Technical Forum (LETF) gegründet, in dem LEAs von Bundesstaaten und weitere lokale berechtigte Stellen sowie 15 LEAs des Bundes vertreten sind.

7.2.2 Technische Anforderungen

Die Anforderungen an die Carrier zur Vorhaltung CALEA-konformer Technologie und Prozesse sind in dem 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.[107]

Der Standard definiert CALEA-konforme Dienste und Merkmale für Netzbetreiber und Hersteller im Bereich drahtgebundener, mobiler und Breitband-Kommunikationstechnologie sowie Schnittstellen zwischen LEAs und den verpflichteten Unternehmen.

Der aktuelle Standard vom Mai 2000 berücksichtigt die Forderungen der FCC aus dem Jahr 1999,[108] die nach Veröffentlichung der ersten Version von J-STD-025 folgende zusätzlichen Anforderungen in der sog. „Punch List" stellte, nachdem sie den ursprünglich von den Unternehmen entwickelten Standard als unzureichend bewertet hatte:

- Möglichkeit der Überwachung des gesamten Inhalts von Konferenzschaltungen,

---

106 Die CIS hat unter www.askcalea ein Informationsportal für CALEA eingerichtet.

107 Vgl. TIA (2000). Das 200 Seiten starke Dokument behandelt ausführlich alle technischen Anforderungen für die Carrier, um CALEA-Kompatibilität zu erreichen. Es ist öffentlich und kann bei der Organisation gegen geringe Gebühr bestellt werden.

108 Vgl. FCC Third Report and Order 99-230 sowie Order on Remand, FCC 02-108, abrufbar unter http://www.askcalea.net/fccregs.html.

- Identifizierung der aktiven Teilnehmer an einer Schaltung mit mehreren Teilnehmern,
- Zugang zu allen Kommunikationsdaten eines Teilnehmers inklusive aller Informationen über die Nutzung von Merkmalen,
- Benachrichtigung der LEA über Zeichengabeinformationen, die von dem zu überwachenden Anschluss ausgehen oder für diesen bestimmt sind (z.B. wenn ein Telefon klingelt oder besetzt ist),
- Bereitstellung von Zeitangaben, um Kommunikationsdaten und Inhalt miteinander korrelieren zu können,
- Bereitstellung der Ziffern, die vom Teilnehmer gewählt wurden, nachdem der Anruf durchgestellt wurde.

Zur Ermöglichung der Überwachung von Kommunikationsdaten sind die TK-Unternehmen, insbesondere die ISP nach dem „Pen/Trap Statute“ verpflichtet, ein Pen/Trap and Trace Device vorzuhalten sowie einen entsprechenden organisatorischen Prozess zur Überwachung zu etablieren. Die technischen Anforderungen definieren ein Instrument, das „dialing, routing, addressing of signaling information“ erfasst, also alles bis auf den Inhalt einer Kommunikation.[109] Für E-Mail bedeutet dies, dass bis auf die Betreffzeile und den Inhalt einer Nachricht alle relevanten Daten an die berechtigten Stellen ausgeleitet werden müssen. Voice-Mail kann ebenfalls nach dem „Pen/Trap Statute“ überwacht werden.

7.2.3 Organisatorische Anforderungen

Weder der Standard von J-STD-025-A noch die „Punch List“ enthalten Angaben zu organisatorischen Anforderungen.

In CALEA ist jedoch ausdrücklich gefordert, dass jeder Carrier gewährleisten muss, dass alle Arten von TK-Überwachungsmaßnahmen nur dann aktiviert werden können, wenn eine entsprechende Anordnung oder andere Genehmigung vorliegt. Das Personal muss sich dabei an gegebenenfalls von der FCC erlassene Verordnungen halten (47 U.S.C. 1004 „Systems Security and Integrity (SS&I)“).

109 Definiert in 18. U.S.C. 3127(4).

Die FCC hat dementsprechend organisatorische Sicherheitsregelungen erlassen, die im Wesentlichen die folgenden Punkte umfassen:[110]

- Der Carrier soll einen qualifizierten und erfahrenen Mitarbeiter mit der Durchführung der Maßnahmen beauftragen, welcher darauf achtet, dass die Überwachung unter Befolgung der gesetzlichen Vorgaben durchgeführt wird.

- Außerdem soll der Carrier Regeln und Prozesse schriftlich verbindlich festlegen. Diese sollen umfassen: die Erklärung, dass Mitarbeiter Überwachungen nur durchführen, wenn eine entsprechende Anordnung vorliegt; eine Definition, wann ein Mitarbeiter davon ausgehen kann, dass eine solche Anordnung vorliegt; eine detaillierte Beschreibung, wie und für wie lange Protokolle der Maßnahmen aufbewahrt werden. Außerdem sollen der Name des verantwortlichen Mitarbeiters, die nötigen Informationen für die LEA, wie dieser „7/24“ zu kontaktieren ist sowie eine Erklärung vorgelegt werden, dass das Unternehmen jede nicht-autorisierte Weitergabe von Kommunikationsinhalten und –daten an dazu nicht befugte Personen und jede nicht-autorisierte Überwachung umgehend den Strafverfolgungsbehörden melden wird.

- Des weiteren ist der Carrier dazu verpflichtet, Protokolle über die von ihm durchgeführten TK-Überwachungsmaßnahmen zu führen. Diese sollen Telefonnummer bzw. sonstige Kennungen; Datum und Zeit des Beginns und des Endes der Überwachung; Name des Vertreters der berechtigten Stelle, der die Anordnung übergibt; Name dessen, der die Anordnung unterzeichnet hat; die gesetzliche Grundlage, auf der die Überwachung erfolgt (FISA, „Title III“, „Pen/Trap Statute“) sowie den Namen des verantwortlichen Mitarbeiters enthalten.

- Die Protokolle müssen von dem Mitarbeiter, der die Überwachung durchführt, unterzeichnet werden. Eine solche Bestätigung muss möglichst sofort, zumindest aber so zeitnah wie möglich erstellt werden. Der Carrier erfüllt die Anforderungen an die Protokollführung, wenn der verantwortliche Mitarbeiter das Protokoll unterzeichnet und zusammen mit der Anordnung sowie ggf. weiteren Anmerkungen ablegt.

- Die Protokolle müssen für eine angemessene Zeit aufbewahrt werden. Die Entscheidung darüber, wie lange die Daten aufbewahrt werden, ist dem Carrier überlassen.

---

110 Vgl. dazu Second Order on Reconsideration FCC 01-126 sowie Report and Order FCC 99-11 und Second Report and Order FCC 99-229. Eine Zusammenfassung findet sich in dem Dokument 66 Fed. Reg. 22,446 (2001). Die Dokumente sind abrufbar unter http://www.askcalea.net/fccregs.html. Die Dokumente modifizieren die in den Verordnungen der FCC 47 CFR 64.2103 („Policies and procedures for employee supervision and control“) und 64.2104 („Maintaining secure and accurate records“) enthaltenen, allgemeinen Regelungen bezüglich der Durchführung von TK-Überwachungsmaßnahmen.

- Es liegt in der Verantwortlichkeit des Carriers, die Protokolle vollständig und sorgfältig zu führen. Verstößt er gegen die Vorschriften, können Sanktionen (Geldstrafen) verhängt werden.[111]

Jeder Carrier ist verpflichtet, seine organisatorischen Sicherheitsmaßnahmen der FCC zur Überprüfung vorzulegen.

7.2.4 Ausnahmen

Unter CALEA existieren keine Ausnahmen von einzelnen Verpflichtungen. Wie bereits dargestellt, können die Unternehmen bei der FCC jedoch einen Aufschub der Verpflichtung zur permanenten Vorhaltung von TK-Überwachungstechnik nach CALEA für sich erwirken.

7.2.5 Genehmigungsverfahren für Überwachungsvorkehrungen

Es existiert ein System der Selbstkontrolle und Selbstzertifizierung. Die Industrie kontrolliert das Design und die Implementation von CALEA-Überwachungstechnologie mittels öffentlicher technischer Standards, zurzeit ist dieser Standard J-STD-025-A.

7.3 Voraussetzungen für die Überwachung

7.3.1 Fälle, in denen das Überwachen der TK angeordnet werden kann

In den USA erfolgt die Überwachung der (Tele)-Kommunikation wie in Deutschland bei einem hinreichenden Verdacht („probable cause“[112]) auf schwere Straftaten.

Laut Omnibus Crime Control and Safe Streets Act von 1968 liegt ein hinreichender Grund im Zusammenhang mit mehreren Dutzend Straftaten vor,[113] insbesondere, wenn die Tat mit der Todesstrafe oder einer Gefängnisstrafe von mehr als einem Jahr geahndet werden könnte.

---

111 Diese sind durch den Communications Act von 1934 U.S.C. 503(b) sowie die Verordnung 47 CFR 1.8 geregelt.

112 Diese Forderung ergibt sich aus dem Fourth Amendment zur US-Verfassung: „The right of the people to be secure [...] against unreasonable searches and seizures, shall not be violated [...] but upon probable cause [...]“ (zit. nach Pallasky, A. (2002), S. 222).

113 Vollständige Liste unter 18 U.S.C. Sec. 2516 („Authorization for interception of wire, oral, or electronic communications“).

Im Wesentlichen werden „Wiretaps“ bei Verdacht auf folgende Straftaten durchgeführt:

Verstöße gegen Drogengesetzgebung (rund zwei Drittel der Maßnahmen), sowie Straftaten im Zusammenhang mit

- Glücksspiel,
- Erpressung,
- Mord/Totschlag,
- schwerer Diebstahl/Diebstahl/Raubüberfall,
- Kreditvergehen/Wucher/Erpressung,
- Bestechung,
- Entführung.

Der USA Patriot Act ergänzt die Liste der möglichen Anlässe für Überwachungsmaßnahmen um weitere Straftaten:[114]

- Einsatz von chemischen und Massenvernichtungswaffen,
- grenzüberschreitende Terrorakte,
- finanzielle Transaktionen, die der Unterstützung des Terrorismus dienen,
- materielle Unterstützung von Terroristen oder terroristischen Organisationen.

Besonderheit

Nur das „Wiretapping“, also „Real Time Interception“, unterliegt Beschränkungen hinsichtlich der Anlässe. „Pen/Trap and Trace“ ist nicht auf bestimmte Tatbestände beschränkt.

7.3.2 Genehmigung einer Überwachungsmaßnahme

Jede TK-Überwachungsmaßnahme nach „Title III“ oder „Pen/Trap Statute“ wird von einem Bundesrichter oder einem Richter eines Bundesstaates der Vereinigten Staaten auf Antrag eines Staatsanwalts angeordnet.[115]

---

114 18 U.S.C. 201, zit. nach Pallasky, A. (2002), S. 222.

115 In den USA können 46 Gerichtsbarkeiten TK-Überwachungen anordnen: die Bundesregierung, der District of Columbia, die Virgin Islands und 43 Staaten. Die TK-Überwachungsregelungen in den ein-

In der Begründung für die Überwachung muss dargelegt werden, dass andere Ermittlungen aussichtslos bzw. fehlgeschlagen oder zu gefährlich sind.

Für Durchsuchungen, um beispielsweise Kommunikationsdaten von Kunden oder Rechnungsdaten zu erhalten, ist keine richterliche Anordnung erforderlich.

Ausnahmen sind in dringenden Fällen möglich. Ein TK-Anbieter oder –Anlagenbetreiber kann eine Überwachung vorzeitig vornehmen (auf Grundlage der Ankündigung einer Anordnung oder auf Basis einer Autorisierung einer berechtigten Stelle). Dies ist beispielsweise auf Grundlage des USA Patriot Act möglich, wenn der Anbieter der Auffassung ist, dass ein Schaden kurz bevor steht.

Außerdem darf der ISP Pen/Trap and Trace Devices ohne gerichtliche Anordnung für eigene Zwecke nutzen, wenn dies dem Schutz seiner Kunden dient oder für technische Kontrollen notwendig erscheint.[116]

7.3.3 Möglicher Zeitraum der Überwachung

Eine „Wiretap Warrant“ kann für 30 Tage angeordnet und dann noch einmal für 30 Tage verlängert werden.

Eine „Pen/Trap Order“ kann für bis zu 60 Tage bestehen und einmalig um 60 Tage verlängert werden.

7.3.4 Überprüfung der Rechtmäßigkeit der Maßnahme durch die Verpflichteten

Die Verpflichteten nehmen eine Augenscheinprüfung vor, d.h. sie prüfen, ob es sich um eine von einem Richter unterzeichnete Anordnung handelt und die zu überwachende Person hinreichend identifiziert ist. Handeln sie im „guten Glauben“ – „good faith“ – schützt sie dies ausreichend vor straf- oder zivilrechtlichen Schritten.[117]

---

zelnen Staaten können sich geringfügig von den hier dargestellten bundesweiten Regelungen unterscheiden.

116 Vgl. 18 U.S.C. 3121(b).

117 Vgl. 18 U.S.C. 3124(d), (e).

7.4 Durchführung der Überwachung

7.4.1 Erforderliche Angaben

In der Anordnung muss die zu überwachende Person hinreichend durch „Kennzeichen“ („particularities“) identifizierbar sein bzw. eine technische Kennung angegeben werden, die zu überwachen ist.

7.4.2 Art der zu überwachenden Telekommunikation

Bei einem „Wiretap“ ist jede Art von Telekommunikation auf Anforderung von den TK-Anbietern und –Anlagenbetreibern zu überwachen und an die berechtigten Stellen weiterzuleiten: Inhalt und Kommunikationsdaten.

Die Unterscheidung in der Überwachung von Internet-Kommunikation besteht darin, ob eine Anordnung nach „Title III“ vorliegt, wonach mittels eines „Sniffer“ die gesamte Kommunikation überwacht werden soll oder eine Anordnung nach dem „Pen/Trap Statute“, was bedeutet, dass die Kommunikationsdaten (ohne den Inhalt) an die Strafverfolgungsbehörden übergeben werden sollen.

In Bezug auf E-Mails bedeutet dies, dass auf Grundlage des „Pen/Trap Statute“ die Kommunikationsdaten der Internet-Kommunikation ohne die Betreffzeile der E-Mail überwacht werden dürfen. Die Überwachung der gesamten E-Mail bedarf einer Anordnung nach „Title III“.

7.4.3 Übermittlung an die berechtigten Stellen

Die TK-Überwachung erfolgt in Echtzeit mit einer „real time“-Übermittlung an die berechtigten Stellen, wenn es sich um eine „Wiretap“-Anordnung handelt. Nur wenn eine Überwachung in Echtzeit erfolgt und die Daten unmittelbar an die berechtigten Stellen gelangen, handelt es sich um ein „interception“ nach „Title III“. Dieser Definition hat sich die Mehrzahl der Gerichte in den USA angeschlossen, der Punkt ist jedoch nach wie vor in der juristischen Diskussion umstritten.[118]

Sprache wird über das öffentliche, vermittelte Netz an die berechtigten Stellen übertragen. Daten werden üblicherweise mittels VPN-Verbindungen gesendet.

---

118 Vgl. die Darstellung unter DoJ (2002), Kapitel D.

Data Retention

Datenspeicherung ist gestattet, wenn die berechtigte Stelle dies von den Unternehmen per Anordnung nach „Pen/Trap Statute“ fordert. Die Daten werden mittels eines Speichermediums, z.B. CD-ROM, übergeben bzw. mit der Post versandt.

Gespeicherte Kommunikation kann auf Basis von ECPA 18 U.S.C. 2703(a) von den Strafverfolgungsbehörden beschlagnahmt werden.

7.4.4 Unterschiedliche technische Einrichtungen für verschiedene Überwachungsanforderungen

Für „Wiretaps“ und „Pen/Trap and Trace“ sind jeweils spezifische technische Einrichtungen und organisatorische Prozesse einzuhalten.

Präventive Überwachungen auf Grundlage von FISA beinhalten andere Regelungen für die Genehmigung der Maßnahme. Die verpflichteten Unternehmen erhalten weniger Informationen über die durchzuführende Überwachung. In technischer Hinsicht handelt es sich jedoch um dieselben Vorgänge, so dass das Vorhalten anderer technischer Einrichtungen nicht notwendig ist.

7.4.5 Echtzeit-Überwachung oder Speicherung

Überwachte Kommunikationsinhalte werden unmittelbar an die berechtigten Stellen übertragen.

Data Retention

Datenspeicherung betrifft gespeicherte Kommunikation (wie z.B. E-Mail) und Kommunikationsdaten. Sie wird bei Bedarf vorgenommen. Die Speicherfrist beträgt nicht mehr als 14 Tage. Zweck dieser Speicherung ist es, den Strafverfolgungsbehörden den Zugriff auf benötigte Informationen in Form von Durchsuchungen zu ermöglichen. Des weiteren besteht die Option, Daten für Rechnungszwecke zu speichern. Darüber hinaus existieren keine weiteren Verpflichtungen zur Datenspeicherung.

7.5 Kontroll- und Sanktionsmaßnahmen

7.5.1 Kontrollinstanzen

Der Omnibus Crime Control and Safe Streets Act von 1968 legt fest, dass das Administrative Office of the United States Courts (AO) einen jährlichen Bericht über die Anzahl und die Art der Überwachungen an den Kongress übergeben muss.[119]

Dieser Wiretap Report enthält keine Daten zu den im Rahmen des Foreign Intelligence Surveillance Act (FISA) durchgeführten Maßnahmen. Es werden auch keine Überwachungsmaßnahmen erfasst, bei denen einer der Kommunikationspartner in die Überwachung eingewilligt hat.

7.5.2 Berichtspflichten

Jeder Bundesrichter und alle Richter der Bundesstaaten sind verpflichtet, jede Überwachungsanordnung dem AO zu melden. Der Bericht muss den Namen des anordnenden Richters, den Verdachtstatbestand, die Art des einzusetzenden Überwachungsmediums, den Einsatzort dieses Mediums und die Dauer der Überwachung enthalten. Persönliche Daten des zu überwachenden werden nicht genannt. Staatsanwälte melden darüber hinaus jährlich die beantragten Überwachungsmaßnahmen direkt an das AO.

7.5.3 Statistiken

Die bereitgestellten Statistiken in den Wiretap Reports des AO sind ausführlich und umfassend und enthalten nicht, wie in Deutschland, die Anzahl der überwachten Kennungen, sondern die Anzahl der autorisierten Maßnahmen. Neben den Anordnungen, aufgeschlüsselt nach Bundesgerichten und Gerichten der einzelnen Staaten, werden auch die Kosten pro Überwachung, die Art der Überwachung und die Erfolgsquote veröffentlicht. Ebenso wird erfasst, in welchen Fällen die Verschlüsselung von Telekommunikation den Erfolg der Überwachungsmaßnahme behindert hat. Die Statistiken über die erfolgten Verurteilungen, zu denen eine elektronische Überwachung beigetragen hat, gehen zurück bis auf das Jahr 1991.[120]

Im Kalenderjahr 2001 wurden 1.491 Überwachungsmaßnahmen durchgeführt, was eine Steigerung von 25 Prozent gegenüber dem Vorjahr bedeutet (vgl. Tabelle 7-2). In 16

---

119 Der Wiretap Report ist abrufbar unter www.uscourts.gov (Administrative Office of the United States Courts (2002): Report of the Director of the AO on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications, May 2002).

120 Zum Vergleich: In den USA leben rund 287,6 Mio. Menschen.

der zu überwachenden Fälle wurde Verschlüsselungstechnik eingesetzt. In keinem dieser Fälle behinderte dies dem Report zufolge die Aufdeckung von Straftaten.

Die Statistik enthält nicht die Maßnahmen nach „Pen/Trap Statute“ sowie Beschlagnahmung von E-Mails oder Anordnungen nach FISA. Insofern ist die im Vergleich zur Bevölkerung sehr niedrige Anzahl von „Wiretaps“ in den USA zu relativieren.

Tabelle 7-2: Autorisierte Überwachungsmaßnahmen in den USA nach 18 U.S.C. 2519 (1991 – 2001)

Jahr	Autorisierte Überwachungen
1991	856
1992	919
1993	976
1994	1.154
1995	1.058
1996	1.149
1997	1.186
1998	1.329
1999	1.350
2000	1.190
2001	1.491

Quelle: Wiretap Report 2002 (Administrative Office of the United States Courts (AO) (2002)) (Die Zahlen geben die Anzahl der Kommunikationsinhalte-Überwachungsmaßnahmen ohne Pen/Trap and Trace Maßnahmen wieder)

Im Durchschnitt waren 86 Personen von einer Maßnahme betroffen. Es wurden im Mittel jeweils 1.565 Kommunikationsvorgänge erfasst. Rund 333 abgefangene Kommunikationsvorgänge pro installierter Abhöreinheit ergaben einen entscheidenden Beweis. 21 Prozent der Überwachungsanordnungen haben zur Strafverfolgung entscheidend beigetragen.

Entsprechend der Formulierung in der Gesetzgebung werden über die Anordnungen nur die Orte („locations“) der Durchführung der Überwachungsmaßnahme statistisch erfasst, nicht die Art der Anschlüsse oder Art und Anzahl von Kennungen. Im aktuellen Wiretap Report des AO werden folgende Arten von Überwachungsmaßnahmen für 2001 genannt:

Überwachung von

- Mobilfunkgeräten (Portable Device) (68 Prozent der Maßnahmen),
- Wohnungen (Personal Residence) (14 Prozent der Maßnahmen),
- kombinierte Überwachungen (8 Prozent der Maßnahmen),
- andere (6 Prozent der Maßnahmen),
- Geschäftsräume (Business) (4 Prozent der Maßnahmen),
- Roving Wiretaps[121] (1 Prozent der Maßnahmen),
- nicht spezifiziert (0,1 Prozent der Maßnahmen).

Die Art der Straftaten, in deren Zusammenhang eine richterliche Anordnung erfolgt ist, werden im jährlichen Bericht des AO aufgeführt. Laut Wiretap Report 2001 werden die Mehrzahl der Überwachungsmaßnahmen im Zusammenhang mit dem Verdacht auf Verstöße gegen die Drogengesetze (78 Prozent) durchgeführt. Danach folgen Straftaten im Zusammenhang mit Glücksspielen (5 Prozent), Erpressung (5 Prozent), Mord/Totschlag (3 Prozent), schwerer Diebstahl/Diebstahl/Raubüberfall (3 Prozent), Kreditvergehen/Wucher/Erpressung (2 Prozent), weitere (3 Prozent), Bestechung (0,01 Prozent), Entführung (0,01 Prozent).

Im jährlichen Wiretap Report werden auch die Kosten für Überwachungsmaßnahmen dargelegt. Demzufolge kostete im Jahr 2001 eine Abhörmaßnahme des Bundes im Durchschnitt 33.650 US-Dollar, eine Maßnahme der jeweiligen Bundesstaaten 74.207 US-Dollar.[122]

Die präventiven Überwachungsmaßnahmen nach FISA werden nur summarisch dokumentiert. Im Jahr 2001 wurden 934 Anträge auf Durchsuchung sowie elektronische Überwachung von dem zuständigen Foreign Intelligence Surveillance Court genehmigt. Zwei Anweisungen und zwei Anordnungen wurden modifiziert, kein Antrag wurde abgelehnt.[123]

---

121 Überwachungen, die mit dem zu Überwachenden „umherwandert“ (to rove).

122 Zahlen wurden auf der Basis der Maßnahmen berechnet, für die Kosten angegeben wurden (89 Prozent der Fälle).

123 Vgl. Brief des Acting Attorney General an den AO v. 29.04.2002, abrufbar unter http://fas.org/irp/news/2002/04/fisa01.html.

7.5.4 Sanktionen

Sanktionen sind im Rahmen des allgemeinen Strafrechts sowie des Zivilrechts vorgesehen. Bei Verstößen gegen die Verordnungen der FCC können Strafen gemäß der vorgesehenen Sanktionen im Rahmen des Communications Act von 1934 verhängt werden.

7.6 Kosten

7.6.1 Bewertung des Aufwands durch die Verpflichteten

Wie in anderen G7-Staaten auch beurteilen die TK-Anbieter und –Anlagenbetreiber und insbesondere die Carrier, die zur permanenten Vorhaltung von technischen Einrichtungen verpflichtet sind, die TK-Überwachung als einen erheblichen Kostenfaktor. Da in den USA Aufwandsentschädigungen in relevanter Höhe gezahlt werden, erscheinen die Proteste jedoch wie in Frankreich und Italien eher moderat. Zu unterscheiden sind Kostenerstattungen im Rahmen von CALEA[124] und allgemeine Kostenerstattungen auf Basis der Regelungen des Criminal Code.

7.6.2 Kostenübernahme und Aufwandsentschädigungen

Der Kongress hat bisher rund 500 Mio. USD für das Zahlen von Aufwandsentschädigungen für den Einsatz von CALEA-konformer Technologie an die verpflichteten Unternehmen bewilligt.[125] Um die Zahlungen abzuwickeln, wurde der „Telecommunications Carrier Compliance Fund (TCCF)“ etabliert. In diesen Fond zahlen die berechtigten Stellen gemäß eines bestimmten Schlüssels ein. Das Justizministerium ist verpflichtet, dem Kongress halbjährlich über die Kostenerstattungen zu berichten. Aktuelle Zahlen wurden im März 2002 publiziert.[126] In dem Bericht wird angedeutet, dass die zur Verfügung stehenden Mittel voraussichtlich nicht ausreichen werden.

Das FBI, das mit der technischen Umsetzung der CALEA-konformen Anforderungen beauftragt ist, hat mit fünf Herstellern und bestimmten verpflichteten Carriern (Bell Atlantic, GTE Communications Systems, Nextel, Loretto Telephone Company, Farmers

---

124 Nach CALEA 47 U.S.C 1008, spezifiziert in der Verordnung 28 CFR 100 (DoJ, Cost recovery regulations, Communications Assistance for Law Enforcement Act of 1994, Revised as of July 1, 2001, teilweise abrufbar unter http://lula.law.cornell.edu/cfr/).

125 CALEA 47 U.S.C. 1009.

126 Vgl. DoJ/OIG (2002). Der Bericht ist abrufbar unter http://www.usdoj.gov/oig/audit/0214/index.htm. Detaillierte Informationen zum Bereich Kostenerstattungen sind auch im jährlichen Bericht des Justizministeriums an den Kongress enthalten, vgl. FBI / DoJ (2001).

Telephone Company) Vereinbarungen[127] geschlossen, die den Einsatz von spezifischer Software befördern sollen. Im Rahmen dieser Vereinbarung werden den Unternehmen Kosten für den Erwerb von „Right-to-use (RTU)"-Lizenzen erstattet. Das FBI hat laut Bericht des DoJ bisher 275 Mio. USD für diese Lizenzen gezahlt und 122 Mio. USD an Kostenerstattungen an die Carrier gewährt (Stand Dezember 2001). Die Zahlungen an die Carrier verteilen sich wie folgt auf Lizenzen folgender Hersteller:

- Lucent Technologies: 170 Mio. USD
- Nortel Networks: 102 Mio. USD
- Motorola: 55 Mio. USD
- Siemens AG: 40 Mio. USD
- AG Communications: 30 Mio. USD

Diese Hersteller decken zusammen mehr als 90 Prozent des von den Carriern in den USA eingesetzten TK-Equipments ab. Die RTU-Software-Lizenzen beinhalten noch keine Erstattungen für die Implementation dieser Software-Lösungen bei den Carriern. Eine entsprechende Vereinbarung zwischen FBI und Unternehmen ist noch in der Diskussion. Es existieren außerdem keine Vereinbarungen über Zahlungen im Zusammenhang mit Systemmodifikationen und es wurden auch keine solchen Zahlungen geleistet.

Über die Diskussion von Kostenerstattungen im Rahmen von CALEA hinaus stehen den Unternehmen im Rahmen des Criminal Code eine vollständige Erstattung der Kosten für die Durchführung von Maßnahmen zu: „Any provider of wire or electronic communication service, landlord, custodian or other person furnishing such facilities or technical assistance shall be compensated therefor by the applicant for reasonable expenses incurred in providing such facilities or assistance."[128]

Die Unternehmen stellen für die Durchführung einer Maßnahmen eine Rechnung an die berechtigte Stelle, die die TK-Überwachungsmaßnahme angefordert hat. Sie können die tatsächlich anfallenden Kosten („reasonable costs") sowohl für „Wiretaps" als auch für „Pen/Trap and Trace" veranschlagen.

Die Summe kann die Investitions-, Wartungs- und Personalkosten enthalten. Im Durchschnitt beträgt die Kostenübernahme für eine „Wiretap"-Maßnahme nach Schätzungen rund 1.500 USD, häufig für ISP aber auch mehr als 10.000 USD. Wie im Wiretap Report 2001 dargestellt, kostet den Staat die Durchführung einer TK-Überwachungsmaßnahme etwa 60.000 USD, so dass die Zahlung an die TK-Unternehmen nur einen geringen Teil dieser Kosten umfasst.

---

127 Dieser pragmatische Ansatz wurde gewählt, da sich die Bestimmung und Erstattung der tatsächlichen Kosten, die die Carrier aufgrund von CALEA-Verpflichtungen erwarten, als nicht praktikabel erwies.

128 18 U.S.C. 2518(4).

8 Rahmenbedingungen für Lawful Interception in Kanada

In Kanada wurde im Jahr 2002 von der Regierung ein Diskussionsprozess initiiert, bei dem es um „Lawful Access“ zu Daten im Rahmen von Strafverfolgungen geht. Das vom Ministerium der Justiz, dem Solicitor General und dem Industrieministerium vorgelegte Konsultationspapier wird zurzeit kontrovers diskutiert. Bisher bildet das Strafgesetz die Grundlage für Überwachungen aller Art. Zentrales Problem dieser Regelung ist, dass die Bestimmungen bezüglich neuer Technologien unklar sind (z.B. E-Mail-Überwachung) und dass die TK-Anbieter und -Anlagenbetreiber nicht verpflichtet sind, technische oder organisatorische Vorkehrungen für die Durchführung von TK-Überwachungsmaßnahmen zu treffen. Eine Gesetzesnovellierung besitzt angesichts der neuesten terroristischen Bedrohungen hohe Priorität für die Regierung.

8.1 Rechtliche Grundlagen

8.1.1 Grundlagen in der TK-Gesetzgebung

Die Sicherstellung der Überwachbarkeit der Telekommunikation ist in Kanada in verschiedenen Gesetzen geregelt, jedoch nicht in der allgemeinen TK-Gesetzgebung. Zurzeit existieren z.B. keine Vorschriften in den TK-Lizenzen oder anderen Regelungen, die von den TK-Anbietern und -Anlagenbetreibern das Vorhalten von Überwachungseinrichtungen verlangen. Allerdings sind diese Unternehmen durch den Telecommunications Act verpflichtet, die Privatsphäre ihrer Kunden zu schützen.[129] Allen lizenzierten Netzbetreibern ist es nach einer Verordnung der kanadischen Regulierungsbehörde verboten, Kundeninformationen – außer Name, Adresse und Telefonnummer – herauszugeben, ohne dass ein schriftliche Einwilligung des Kunden vorliegt.[130]

Der Radiocommunications Act von 1985 wurde im Jahr 1996 novelliert, um die Mobilfunknetzbetreiber zu verpflichten, technische Möglichkeiten zur Sicherstellung der Überwachbarkeit der Telekommunikation für die Strafverfolgungsbehörden bereitzustellen.

8.1.2 Einschlägige Rechtsvorschriften

Die Sicherstellung der Überwachbarkeit der Telekommunikation bzw. vielmehr die Überwachung im Rahmen der Strafverfolgung im Allgemeinen („Lawful Access“) wird in Kanada durch die folgenden Rechtsvorschriften geregelt:

---

129 Telecommunications Act 1993, c. 38, s. 39, s. 41 (s. EPIC/PI (Eds.) (2002), S. 138).
130 Festgelegt z.B. in Bell Canada Terms of Service, General Tariff Item 10, Article 11.

- Strafgesetzbuch: Criminal Code (R.S. 1985, c. C-46) An Act respecting the Criminal Law (Part VI, Invasion of Privacy;[131] Part XV, Special Procedure and Powers). Dieses Gesetz ist die wichtigste Quelle für die zurzeit geltenden Regelungen in Bezug auf Überwachung. Teil VI bestimmt die Rahmenbedingungen, unter denen private Kommunikation (in Anwesenheit der Kommunikationspartner oder elektronisch vermittelt) überwacht werden darf. Explizite Regelungen für die Telekommunikation sind hier nicht festgehalten. Teil XV regelt Fragen der Durchsuchung und Beschlagnahmung (u.a. auch von Computern).

- Gesetz zur Etablierung des Geheimdienstes: Canadian Security Intelligence Service Act, CHAPTER C-23, An Act to establish the Canadian Security Intelligence Service. Das Gesetz regelt die allgemeinen Überwachungsbefugnisse des Geheimdienstes.

- Wettbewerbsrecht: Competition Act, CHAPTER C-34, An Act to provide for the general regulation of trade and commerce in respect of conspiracies, trade practices and mergers affecting competition. Bei Verstößen gegen das Wettbewerbsrecht besitzt das Competition Bureau ebenso wie Strafverfolgungsbehörden Kompetenzen im Bereich Überwachung, Durchsuchung und Beschlagnahmung. Auch diese Befugnisse sollen im Rahmen der neuen elektronischen Kommunikationsmöglichkeiten erweitert werden.[132]

- Anti-Terrorismus-Gesetzgebung: Anti-Terrorism Act (ATA), Bill C-36 v. 28. November 2001. Das Gesetz erweitert die Befugnisse der allgemeinen Überwachung in Zusammenhang mit dem Verdacht auf terroristische Aktivitäten.

Die Grundlagen in Bezug auf Privatsphäre und Datenschutz bzw. allgemeine Menschen- und Bürgerrechte sind in einer Charta geregelt:

- Canadian Charter of Rights and Freedoms Constitution Act, 1982 (79), Enacted as Schedule B to the Canada Act 1982 (U.K.) 1982, c. 11, April 17, 1982.

Die Kompetenz für den Bereich LI liegt beim Justizministerium. Die Prozesse der Überwachung werden durch das Parlament bzw. Gerichtsentscheide definiert. Die kanadische Regulierungsbehörde CRTC besitzt keinen Einfluss auf Regelungen, die die Durchführung von Überwachungsmaßnahmen betreffen, sie kann jedoch bestimmen, welche Informationen lizenzierte Telefonanbieter den Strafverfolgungsbehörden zur Verfügung stellen müssen (z.B. Telefonnummern und ähnliche Kunden-Adressinformationen).

Lawful Interception wird im Zuge der jüngsten internationalen Diskussion auf G7/G8-Ebene auch in Kanada zu einem vorrangigen politischen Thema. Die kanadische Re-

---

131 In Kraft seit 1974.
132 Zum Beispiel um Straftaten im Zusammenhang mit neuen digitalen Dienstleistungen zu bekämpfen.

gierung hat im Sommer 2002 einen Diskussionsprozess unter der Federführung des Justizministeriums und gemeinsam mit dem Industrieministerium sowie dem Solicitor General initiiert, in dem Fragen der künftigen Regelung von Überwachung geregelt werden sollen. Dazu wurde das Dokument „Lawful Access – Consultation Document“[133] veröffentlicht. Der Konsultationsprozess wurde bis Dezember 2002 verlängert. Mit einer Implementierung neuer Regelungen ist voraussichtlich nicht vor Mitte 2003 zu rechnen. Voraussichtlich werden die Änderungen im Rahmen einer Novellierung des Criminal Code durchgeführt. Die Schaffung einer gesetzlichen Grundlage für LI wird u.a. deshalb forciert, um die Cybercrime Konvention des Europarats ratifizieren zu können.[134]

Im folgenden wird auf die Planungen der kanadischen Regierung zu einer „Lawful Access“-Gesetzgebung Bezug genommen. Auf die derzeit noch geltenden Regelungen wird jeweils vergleichend eingegangen. Kernpunkt der Neuregelung ist die Implementation von Bestimmungen, nach denen jede Art von Telekommunikation – drahtgebunden, drahtlos und Internet-Kommunikation – im Bedarfsfall abgehört werden kann.

8.1.3 TK-Dienste, für die die Überwachbarkeit gewährleistet sein muss

Geregelt ist zurzeit die Durchführung von „electronic surveillance“, d.h. die Überwachung einer nicht-öffentlichen Kommunikation („private“), die entweder mittels elektronischer Kommunikationstechnik oder im Beisein der Kommunikationspartner ohne weitere Hilfsmittel („oral“) stattfindet. Die unklar formulierte Definition von privater Kommunikation als „oral communication“ hat in Kanada zu juristischen Auseinandersetzungen darüber geführt, ob E-Mail-Kommunikation in den Bereich der privaten Kommunikation fällt und damit auf E-Mail-Überwachung die weitergehenden Bestimmungen zum Schutz der Privatsphäre nach Teil VI des Criminal Code zutreffen oder die weniger restriktiven Bestimmungen nach Teil XV (wonach E-Mail im Rahmen von Durchsuchungen und Beschlagnahmungen überwacht werden könnte). In der kanadischen Rechtsprechung finden sich Urteile zu beiden Interpretationsmöglichkeiten.[135] Ziel der neuen Gesetzesänderungen ist es, in diesem Punkt Eindeutigkeit zu schaffen.

Genehmigt wird heute generell eine Audio-Überwachung oder eine Video-Überwachung. Im Antrag auf Überwachung und in der Anordnung werden dann die Mittel für die Überwachung spezifiziert, d.h. hier können dann Arten der TK-Überwachung beantragt werden.

---

133 Department of Justice; Industry Canada and Solicitor General (2002): Lawful Access – Consultation Document, Government of Canada, 25 August 2002.

134 Dies setzt eine gesetzliche Regelung zur TK-Überwachung voraus.

135 Vgl. ebenda, S. 15. Diese Problematik ist auch aus den Regelungen zur TK-Überwachung in Deutschland bekannt, wo Strafverfolgungsbehörden E-Mails nach der StPO und nicht nach den Bestimmungen der TKÜV überwachen.

Die derzeitige Regelung in der Strafgesetzgebung sieht die Überwachbarkeit von Telekommunikation wie folgt vor:

- gesamte Kommunikation (Inhalt und Kommunikationsdaten), dies bezieht sich faktisch auf Sprachkommunikation,
- sog. Pen Register, mit denen die ausgehenden Kommunikationsdaten erfasst werden (vergleichbar einem Einzelverbindungsnachweis),
- sog. Trap and Trace, mit dem die eingehenden Kommunikationsdaten erfasst werden.

Zusätzlich zu der Überwachung von Kommunikation besteht für die Strafverfolgungsbehörden die Möglichkeit, im Rahmen von Durchsuchungsbefehlen und Beschlagnahmungen von (Kommunikations-)Daten und -Inhalten, die in Computern gespeichert sind, Kenntnis zu erlangen.

Ziel der „Lawful Access“-Gesetzesplanung ist es, die rechtlichen Voraussetzungen für die Überwachbarkeit der gesamten elektronischen Kommunikation, d.h. von

- „wireless“,
- „wireline“,
- und Internet-Kommunikation

zu schaffen. Das bedeutet für die Anbieter solcher Dienste, dass sie in Zukunft technische Vorkehrungen zu treffen haben, um die Überwachbarkeit zu gewährleisten.

Data Retention

Im Rahmen der Gesetzesnovellierung wird diskutiert, dass Internet Service Provider alle Logfiles für bis zu sechs Monate speichern müssen.

8.1.4 Zweck der Überwachung

Nach kanadischem Recht besteht das Ziel der Überwachung von privater Kommunikation darin, die Untersuchung, Aufdeckung, Verhinderung und Verfolgung von Straftaten zu unterstützen. Besondere Bedeutung kommt der Überwachung in Bezug auf die Bekämpfung von organisiertem Verbrechen, insbesondere im Bereich Drogenhandel und damit zusammenhängenden Delikten wie Geldwäsche und Schmuggel, zu.

Entgegen den Gepflogenheiten im Vereinigten Königreich dürfen Ergebnisse der Kommunikationsüberwachung in Gerichtsverfahren als Beweise genutzt werden. Die Daten werden den Beschuldigten und ihren Verteidigern zugänglich gemacht.

8.1.5 Unterschiede zwischen individuellen Überwachungsmaßnahmen der Strafverfolgungsbehörden und denen der Sicherheitsbehörden

Der Canadian Security Intelligence Service Act regelt die Befugnisse der Geheimdienste, Kommunikation zum Zweck der Gewährleistung der nationalen Sicherheit zu überwachen. Auch in diesen Fällen ist eine richterliche Anordnung notwendig, die für den durchführenden Canadian Security Intelligence Sercie (CSIS) nur ein Bundesrichter am Federal Court of Canada erteilen darf.

Das Anti-Terrrorismus-Gesetz Bill C-36 änderte den bestehenden National Defence Act dahingehend, dass die Behörde Communications Security Establishment (CSE) nicht nur Kommunikation im Ausland, sondern auch Kommunikation zwischen Kanadiern und Ausländern überwachen darf. Die Erlaubnis dazu erteilt jeweils der Minister of National Defence.

8.2 Verpflichtungen für die TK-Anbieter und Betreiber von TK-Anlagen

8.2.1 Kreis der Verpflichteten

Zurzeit ist nicht explizit definiert, welche Verpflichtungen TK-Anbieter und -Anlagenbetreiber hinsichtlich der Unterstützung bei Überwachungsmaßnahmen haben und zwar sogar dann nicht, wenn eine Autorisierung zur Überwachung seitens der Strafverfolgungsbehörden vorliegt.[136]

In Zukunft sollen alle Anbieter von drahtgebundenen und drahtlosen TK-Diensten sowie Internet-Diensten verpflichtet sein, die Überwachung von Kommunikation zu ermöglichen. Die Anforderungen im Konsultationspapier beziehen sich sowohl auf Inhalt als auch auf Kommunikationsdaten.

8.2.2 Technische Anforderungen

Derzeit existieren keine gesetzlichen Grundlagen, die die Anforderungen an die TK-Anbieter und -Anlagenbetreiber hinsichtlich der Vorhaltung von technischen Anlagen zur Überwachung festlegen. Es ist vom Department of Justice geplant, allgemeine Funktionsanforderungen festzuschreiben. Eine der Regierung auf Empfehlung des Ministry of Industry und des Solicitor General noch zu benennende Behörde soll diese spezifizieren. Der Fokus der Diskussion liegt derzeit auf folgenden Fragen:

---

136 Vgl. ebenda, S. 7.

- Wie kann eine technische Vorrichtung bei den Verpflichteten installiert werden, um das Überwachen zu ermöglichen? Welche Kapazitäten für die gleichzeitige Überwachung von mehreren Anschlüssen sind vorzuhalten?
- Welches sollen die Bedingungen für die Gewährleistung einer umfassenden Sicherheit von Überwachungsmaßnahmen sein?
- Wie soll die zu überwachende Telekommunikation an die Behörden weitergegeben werden?
- Welche Vorkehrungen sind zu treffen hinsichtlich der Qualifikation, Zuverlässigkeit und des Einsatzes von Mitarbeitern?
- Sollen die Verpflichteten Kostenerstattungen oder Aufwandsentschädigungen erhalten?

8.2.3 Organisatorische Anforderungen

Auch in Bezug auf organisatorische Anforderungen existieren in Kanada derzeit keine gesetzlichen Vorschriften. Diese werden voraussichtlich gemeinsam mit den technischen Anforderungen definiert werden.

8.2.4 Ausnahmen

Es wird im Konsultationspapier vorgeschlagen, Ausnahmen für bestimmte Anforderungen zuzulassen. Details wurden noch nicht definiert. Angedacht ist, dass die Regierung die Kompetenz für die Gewährung von Ausnahmen an das Ministry of Industry und den Solicitor General weitergibt und diese im Einzelfall prüfen, ob und welche Sonderregelungen für ein Unternehmen greifen. Innerhalb der Prüfungsperiode wären vom Antragsteller keine Sanktionen zu befürchten.

8.2.5 Genehmigungsverfahren für Überwachungsvorkehrungen

Die Befolgung der Vorschriften soll kontrolliert werden. In welcher Form dies geschieht, steht noch nicht fest.

8.3 Voraussetzungen für die Überwachung

8.3.1 Fälle, in denen das Überwachen der TK angeordnet werden kann

Überwachungsmaßnahmen dürfen von einem Richter angeordnet werden, wenn der Verdacht besteht, dass ein Verstoß gegen den Criminal Code oder ein anderes Gesetz vorliegt, der einen Eingriff in die Privatsphäre rechtfertigt. Dies geschieht beim Verdacht auf:

- strafbare Handlungen im Zusammenhang mit Drogen bzw. Betäubungsmitteln. Dieser Bereich macht den weitaus größten Teil der gewährten Anordnungen aus.
- Verstößen gegen Import- und Exportbestimmungen,
- Verstößen gegen Zoll- und Abgabenbestimmungen,
- Verstößen gegen die Immigrationsbestimmungen,
- Kapitalverbrechen.[137]

8.3.2 Genehmigung einer Überwachungsmaßnahme

Zurzeit wird eine Maßnahme nach dem Criminal Code Part VI Sec. 185 („authorisation“, vergleichbar einer Überwachungsanordnung) und nach Sec. 487.01 („warrant“, vergleichbar einem Durchsuchungsbefehl) genehmigt. Voraussetzung ist, dass[138]

- der polizeiliche Ermittler eine eidesstattliche Erklärung abgibt darüber, dass eine „authorisation“ oder ein „warrant“ notwendig ist. Er muss plausible Gründe dafür nennen, warum eine Überwachung der Kommunikation für die Strafverfolgung notwendig ist.
- Der Ermittler ist verantwortlich für die rechtmäßige Durchführung und dafür, dass das Vergehen schwerwiegend genug dafür ist, um eine Überwachung oder Durchsuchung zu rechtfertigen und nicht bereits genügend Beweise vorliegen.
- Der Richter, der den Antrag auf „authorisation“ oder „warrant“ entgegennimmt, muss davon überzeugt sein, dass keine anderen Wege der Ermittlung sinnvoll sind.

---

137 Eine ausführliche Auflistung findet sich bei Department of the Solicitor General of Canada (2001), S. 7ff.

138 Vgl dazu Criminal Code Part VI und Part XV sowie Department of the Solicitor General of Canada (2001), S. 2.

In der Praxis stellt nur der Solicitor General oder ein von ihm Bevollmächtigter einen Antrag auf Überwachung bzw. Durchsuchung. Beispielsweise sind einige hochrangige Polizeibeamten vom Solicitor General bevollmächtigt, in dringenden Fällen kurzfristig Anträge zu stellen. Polizeiliche Ermittler benötigen eine schriftliche Genehmigung ihres Vorgesetzten, bevor sie sich an einen der Bevollmächtigten wenden. Die Bevollmächtigten, die einen Antrag gestellt haben, werden im jährlichen Bericht des Solicitor General namentlich genannt.

Es bleibt dem Richter überlassen, Einschränkungen der Überwachung im Hinblick darauf zu treffen, wer wie, wann und wo überwacht sowie welche Art von Überwachung vorgenommen wird. Beispiele sind Anforderungen an die Durchführung von Überwachungen, bei denen Vertrauensverhältnisse, z.B. zwischen Rechtsanwalt und Mandant betroffen sind.

Keine Genehmigung ist für Überwachungen notwendig, wenn einer der Kommunikationspartner eingewilligt hat oder die Überwachung aus technischen Gründen erforderlich ist.

Die Herausgabe von Kunden- bzw. Rechnungsdaten bedarf seit 2001 nicht mehr einer richterlichen Anordnung. Die Änderung, angestoßen durch den Personal Information Protection and Electronics Documents Act (PIPEDA), wurde durch die kanadische Regulierungsbehörde CRTC implementiert, die die „Terms of Service“ für Bell Canada entsprechend veränderten. Sog. Reverse Directory Information (Suche nach Namen bei bekannter Telefonnummer) sind jetzt ebenfalls ohne Anordnung möglich.

Für Anordnungen nach dem Anti-Terrorism Act ist ein weniger aufwändiger Beantragungsprozess vorgesehen. Es ist für die Maßnahmendurchführung nach diesem Gesetz nicht notwendig nachzuweisen, dass es sich bei der Kommunikationsüberwachung um das letztmögliche Mittel handelt.

Data Retention

Künftig ist geplant, zwei weitere Genehmigungsarten im Rahmen von „Lawful Access“ – neben der Autorisierung zur Überwachung und der Anordnung von Durchsuchungen - zuzulassen. Es handelt sich um[139]

- „Preservation order“: Anordnungen, die einen Anbieter verpflichten, Daten im Zusammenhang mit bestimmten Transaktionen oder Personen zu speichern,[140]
- „General production order“: Anordnung, die einen Anbieter verpflichtet, bestimmte Daten an die Strafverfolgungsbehörden weiterzugeben. Es handelt sich dabei um

---

139 Vgl. Privacy Commissioner of Canada (2002).

140 Es ist scheinbar keine allgemeine Datenspeicherungsverpflichtung angedacht. Die vorgeschlagenen Speicherzeiträume belaufen sich auf 90, 120 oder 180 Tage.

eine Art von Anordnung ähnlich der „Durchsuchung“. Die Anwesenheit eines Polizeibeamten ist für diese „Durchsuchung“ jedoch nicht notwendig, d.h. sie könnte online erfolgen.

- „Specific production order“: Anordnung, die einen Anbieter verpflichtet, Kommunikationsdaten („traffic data“) an die Strafverfolgungsbehörden weiterzugeben.
- Evtl. weitere „Specific production order“: Anordnung, die die Herausgabe von Kunden- und Rechnungsdaten betrifft.

8.3.3 Möglicher Zeitraum der Überwachung

Nach dem Criminal Code wird eine Überwachung heute für zunächst bis zu 60 Tagen genehmigt. Verlängerungen von bis zu 60 Tagen sind möglich, wenn die Begründung für die Notwendigkeit der Überwachung weiterhin zutrifft.

In dringenden Fällen darf die Überwachung kurzfristig für 36 Stunden durch einen Richter angeordnet werden, ohne dass der Solicitor General persönlich einen Antrag auf Überwachung gestellt hat. In diesen Ausnahmefällen kann ein höherrangiger Polizeibeamter die Maßnahme beantragen.

Im Rahmen der Bekämpfung von terroristischen Aktivitäten im Rahmen des Anti-Terrorism Act kann eine Überwachungsanordnung für ein Jahr gewährt werden.

8.3.4 Überprüfung der Rechtmäßigkeit der Maßnahme durch die Verpflichteten

Es existiert keine derartige Verpflichtung. Es existieren auch keine fest definierten Prozesse, die festlegen, was den TK-Anbietern und –Anlagebetreibern vorgelegt werden muss. In der Praxis wird die Anordnung vorgelegt. Sec. 188.2 des Criminal Code schützt diejenigen vor Strafen, die bei Überwachungsmaßnahmen in dem guten Glauben handeln, die Maßnahme sei autorisiert und damit legal.

8.4 Durchführung der Überwachung

In Ermangelung gesetzlicher Vorgaben für eine Verpflichtung der Unternehmen, bestimmte Vorkehrungen zu treffen, haben die kanadischen Strafverfolgungsbehörden nach Aussagen von Experten mit den TK-Anbietern und –Anlagebetreibern vertrauliche Vereinbarungen zur Sicherstellung der Überwachbarkeit der Telekommunikation getroffen. Diese Vereinbarungen beruhen, wie bereits dargestellt, heute nicht auf einer gesetzlichen Grundlage bzw. veröffentlichten Verordnungen oder Codes of Practice. Eine solche Basis soll erst mit der geplanten rechtlichen Regelung von „Lawful Access“ ge-

schaffen werden. Die streng vertraulichen, derzeit geltenden Regelungen sind nicht öffentlich zugänglich.

Es wurde jedoch betont, dass die Kommunikation heute in Echtzeit überwacht wird. Dies gilt auch für die Datenkommunikation, allerdings ist dann eine Nachbearbeitung der Daten notwendig. Gespeicherte Daten werden in erster Linie im Rahmen von Durchsuchungen und Beschlagnahmungen überwacht. Im Rahmen der Überwachung von Sprachtelefonie wird der Inhalt sowie die Kommunikationsdaten erfasst.

8.5 Kontroll- und Sanktionsmaßnahmen

8.5.1 Kontrollinstanzen

Es ist die Aufgabe des Department of the Solicitor General gemäß Criminal Code Sec. 195,[141] die Praxis der Überwachung zu kontrollieren und dazu jährliche Berichte an das Parlament zu übergeben.[142]

Die Überwachung durch den Canadian Security Intelligence Service (CSIS) kontrolliert das Security Intelligence Review Committee (SIRC).

Besonderheit

Nach Criminal Code subsection 196(1) ist der Solicitor General verpflichtet, eine Person 90 Tage nach Ergehen der Autorisierung zur Überwachung schriftlich darüber zu informieren, dass sie Objekt einer Überwachungsmaßnahme war. Der Zeitraum für das Übersenden der Mitteilung kann auf bis zu drei Jahre ausgedehnt werden, wenn es sich um die Überwachung einer kriminellen Vereinigung handelt.

8.5.2 Berichtspflichten

Die vom Solicitor General bevollmächtigten Personen, die einen Antrag auf Überwachung stellen dürfen, müssen die entsprechenden Angaben an den Solicitor General weitergeben. Ebenso sind die Polizeieinheiten, die Anträge an diese Bevollmächtigten stellen, verpflichtet, Angaben darüber für den jährlichen Kontrollbericht weiterzuleiten.

---

141 Vgl. www.sgc.gc.ca.

142 Der Begriff ist aus dem Rechtssystem des Vereinigten Königreichs übernommen und wird mit „zweiter Kronanwalt“ übersetzt.

8.5.3 Statistiken

Der Solicitor General sowie das SIRC erstellen jährlich einen Bericht zu den durchgeführten Überwachungsmaßnahmen (vgl. Tabelle 8-1).

Tabelle 8-1: Telekommunikations-Überwachungs-Anordnungen in Kanada 1995 - 2000

	FY1995	FY1996	FY1997	FY1998	FY1999	FY2000
Part VI Criminal Code (Strafverfolgung)	998	693	1420	737	736	k.A
CSIS s. 21 Anordnungen (strategische Überwachung)	32	125	72	84	76	56
CSIS Anordnungen (Erneuerungen)	180	163	153	163	181	150

Quelle: Security Intelligence Review Committee. SIRC Report 2000-2001; Solicitor-General Canada (zit. nach Surtees, L.; Chaisatien, W. 2002) (ohne Pen Register und Trap and Trace Überwachung)

Die Tabelle zeigt die Gesamtzahl der Überwachungen, ohne Unterscheidung zwischen Audio- und Video-Überwachung.[143] Der Bericht des Solictor General belegt jedoch, dass die Methode der TK-Überwachung am weitaus häufigsten genutzt wird. Von 1.143 einzelnen Überwachungsaktionen im Rahmen der 736 genehmigten Anordnungen im Jahr 1999 wurde in 83 Prozent der Aktionen die Methode der TK-Überwachung gewählt.[144]

In Kanada wird der Erfolg von Überwachungsmaßnahmen ausgewertet und veröffentlicht. Im Jahr 1999 konnten beispielsweise 348 Personen mit Unterstützung von Überwachungsmaßnahmen festgenommen werden, im Jahr 2000 waren es 207.[145]

8.5.4 Sanktionen

Da keine gesetzlichen Verpflichtungen für die TK-Anbieter und Anlagenbetreiber bestehen, technische Überwachungseinrichtungen vorzuhalten und organisatorische Vorkehrungen zu treffen, scheint es auch keine spezifischen Sanktionen in diesem Bereich zu geben. Belege dafür konnten nicht gefunden werden, es scheint jedoch plausibel, dass

---

143 Zum Vergleich: In Kanada leben rund 30 Mio. Menschen.
144 Vgl. Department of the Solicitor General of Canada (2001), S. 11.
145 Ebenda, S. 12.

auch in Kanada die Unternehmen wie jeder Bürger verpflichtet sind, an der Aufklärung von Straftaten mitzuwirken. Regelungen zu diesem Punkt finden sich im Criminal Code s. 21 und ss. 23, 463 wonach sich jemand strafbar macht, der etwas tut bzw. unterlässt und dadurch dazu beiträgt, dass eine Straftat begangen wird.[146]

8.6 Kosten

8.6.1 Bewertung des Aufwands durch die Verpflichteten

Auch in Kanada hat die im Konsultationspapier formulierte Anforderung des Justizministeriums an die TK-Anbieter und –Anlagenbetreiber, künftig technische Überwachungseinrichtungen vorzuhalten und organisatorische Vorkehrungen zu treffen, kontroverse Diskussionen über die zu erwartenden Kosten ausgelöst.

8.6.2 Kostenübernahme und Aufwandsentschädigungen

Es ist im Rahmen der neuen Gesetzgebung geplant, dass die Unternehmen die gesamten netzseitigen Kosten für Überwachungseinrichtungen tragen müssen, wenn sie neue Dienste implementieren sowie dann, wenn sie ein Upgrade bestehender Systeme vornehmen. Gefordert ist eine „basic intercept capability“, also eine Grundausstattung, die aber noch nicht näher definiert wurde.

Für notwendige Änderungen an bestehenden Systemen sollen die Unternehmen die Kosten nicht selbst tragen. In dem Konsultationspapier werden jedoch keine konkreten Aussagen dazu gemacht, wie die Kosten gedeckt werden oder ob evtl. für bestehende Systeme zunächst keine technischen Einrichtungen dauerhaft vorgehalten werden müssen.

---

146 Criminal Code s. 21(1)(b), vgl. Elder, D. (2002), S. 5f.

9 Rahmenbedingungen für Lawful Interception in Japan

Im August 1999 hat Japan als letzter der G7-Staaten ein Gesetz zu Lawful Interception verabschiedet. Manche sahen dies als notwendigen, längst überfälligen Schritt, der auch von internationalen Bündnispartnern immer mehr gefordert wurde, andere kritisieren dies als schrittweise Demontierung der Bürgerrechte und des in Japan kulturell hochstehenden und fest verankerten Fernmeldegeheimnisses.[147] Aufgrund der noch geringen Erfahrung mit der Umsetzung des Gesetzes liegen kaum Informationen vor. Insbesondere Verordnungen und Richtlinien zur praktischen Umsetzung fehlen bisher.

Die weiteren Ausführungen stützen sich im Wesentlichen auf die Aussagen von Experten und auf Sekundärliteratur, da offizielle Übersetzungen der einschlägigen Gesetze aus dem Japanischen nicht vorliegen.

9.1 Rechtliche Grundlagen

9.1.1 Grundlagen in der TK-Gesetzgebung

In Japan enthält die TK-Gesetzgebung keine Regelungen zum Bereich Lawful Interception. Relevant für den Bereich TK-Überwachung ist jedoch die Regelung des TKG, Art. 4, wonach Unternehmen grundsätzlich das Fernmeldegeheimnis zu wahren haben.

Das Fernmeldegeheimnis genießt darüber hinaus Verfassungsrang (Jap. Verfassung Art. 21: „Es soll weder Zensur ausgeübt, noch soll das Geheimnis jedweder Kommunikation verletzt werden“ [eigene Übersetzung aus dem Englischen.]).[148] Eine Verfassungsklage im Jahr 1999 gegen das Gesetz hatte jedoch keinen Erfolg. Der Entscheidung lag die Auffassung zugrunde, dass in Bezug auf die Strafverfolgung die Gemeinschaftsinteressen über den Interessen des Einzelnen auf Wahrung seines Fernmeldegeheimnis zu stellen sind.

9.1.2 Einschlägige Rechtsvorschriften

In der japanischen Verfassung genießt das Fernmeldegeheimnis einen hohen Stellenwert.[149] Dies wird vor allem darin deutlich, dass bis vor kurzem keine TK-Überwachungsmaßnahmen in der Strafverfolgung eingesetzt wurden. Entsprechend

---

147 Vgl. Gilmer, L. R. (2002).

148 Vgl. ausführlich die juristische Darstellung bei Gilmer, L. R. (2002), S. 910ff.

149 Vgl. Art. 21: „No censorship shall be maintained, nor shall the secrecy of any means of communication be violated“. Das japanische Verfassungsgericht hat eine Klage bezüglich des CI-Act geprüft und ist zu der Entscheidung gekommen, dass das Gesetz keinen Verfassungsverstoß darstellt, wenn es korrekt angewandt wird.

erwarten Experten zurzeit trotz der Diskussion um Terrorismusbekämpfung keine Ausweitung dieser Maßnahmen.[150]

In Japan ist die Sicherstellung der Überwachbarkeit der Telekommunikation in Bereich der Strafgesetzgebung geregelt. Die entsprechenden Gesetze sind das

- "Law authorizing interceptions of telecommunications in crime investigations" (Law No. 137, 1999)[151] und die
- "Code of Criminal Procedure - CCP" (Strafprozessordnung). Letztere spezifiziert die Bestimmungen des Gesetzes.[152] Relevant sind Art. 100 (Beschlagnahmung von Briefen durch Richter), Art. 222 (Beschlagnahmung von Briefen und Telegrammen durch Staatsanwälte, höherrangige Kriminalpolizeibeamte sowie Art. 222-2 (Erweiterung bzw. Änderung des CCP durch den CI-Act).

Zuständig für Lawful Interception ist das Justizministerium.

Weitere Gesetze, z.B. im Rahmen von Terrorismusbekämpfungsgesetzen, wurden bisher nicht erlassen. Ebenso fehlt ein formaler „Code of Practice“ oder eine Verordnung, in der die Verpflichtungen von TK-Unternehmen in Bezug auf die Überwachung geregelt sind.

Das Strafprozessrecht in Japan gilt als unterentwickelt. Daher erscheint aus Sicht mancher Juristen eine grenzüberschreitende Kooperation zur Bekämpfung von organisiertem Verbrechen als äußerst schwierig.[153]

9.1.3 TK-Dienste, für die die Überwachbarkeit gewährleistet sein muss

In Japan ist durch den CI-Act die Überwachbarkeit von folgenden Diensten sichergestellt:

- Sprachtelefonie,
- Fax,
- E-Mail.

---

150 Es gibt Stimmen, die bezweifeln, ob die fehlende gesetzliche Grundlage für LI bedeutet, dass die Polizei bisher keine TK-Überwachungen durchgeführt hat. Ein Skandal, bei dem die Polizei den Vorsitzenden der Kommunistischen Partei abgehört haben soll, ging 1996 durch die japanische Presse. Es konnten jedoch keine eindeutigen Belege für die Überwachung gefunden werden (vgl. Gilmer, L. R. (2002), S. 893). Ein Unternehmen namens Rion behauptet, der japanischen Polizei seit 1957 Überwachungssysteme für Sprachtelefonie zu verkaufen.
Vgl. Wired v. 2.06.1999, http://www.wired.com/news/print/0,1294,19973,00.html.

151 Im weiteren Text Communications Interception Act (CI-Act) genannt.

152 Es existiert zu beiden Gesetzen weder eine offizielle noch eine informelle Übersetzung aus dem Japanischen. Die offizielle, umfassendste Website zu diesem Thema ist unter http://www.moj.go.jp/HOUAN/houan02.html zu finden.

153 Vgl. Gilmer, L. R. (2002), S. 894.

9.1.4 Zweck der Überwachung

Ziel der Überwachung ist die Bekämpfung von schweren Straftaten und vor allem des organisierten Verbrechens. In Japan stellen die Aktivitäten der sog. Yakuza-Mafia, der Sokaiya, die vorrangig auf die Erpressung von Großunternehmen[154] spezialisiert ist sowie die Aum-Sekte[155] eine Bedrohung dar, die man u.a. durch TK-Überwachung bekämpfen will.

9.1.5 Unterschiede zwischen individuellen Überwachungsmaßnahmen der Strafverfolgungsbehörden und denen der Sicherheitsbehörden

Es gibt Hinweise in der Presse dafür, dass die sog. Public Security Police „präventive" TK-Überwachungsmaßnahmen durchführt. Offizielle Belege konnten jedoch nicht gefunden werden. In der japanischen Gesetzgebung wird nicht zwischen individueller oder anderen Überwachungsarten unterschieden.

9.2 Verpflichtungen für die TK-Anbieter und Betreiber von TK-Anlagen

9.2.1 Kreis der Verpflichteten

Art. 11 des CI-Act gestattet es Staatsanwälten und höherrangigen Polizisten, im Rahmen einer richterlichen Anordnung alle TK-Anbieter und -Anlagenbetreiber zur Kooperation bei der Durchführung von Überwachungsmaßnahmen aufzufordern.

9.2.2 Technische Anforderungen

Es bleibt den Strafverfolgungsbehörden überlassen, technische Systeme fallweise zu installieren. CI-Act, Art. 10, legt fest, dass die Behörden die notwendigen Schritte dazu ergreifen. Technische Richtlinien in diesem Zusammenhang sind nicht öffentlich bekannt.

E-Mail-Kommunikation wird mittels einer „Temporary Mailbox" überwacht, die aus einem Speichermedium besteht, welches bedarfsweise von den Strafverfolgungsbehörden installiert wird.[156]

---

154 Angeblich müssen 90 Prozent aller japanischen Unternehmen an die Sokaiya zahlen, vgl. Gilmer, L. R. (2002), S. 907.
155 Weltweit bekannt wurde diese Sekte, als sie einen Giftgasanschlag in der U-Bahn von Tokio verübte.
156 Vgl. Ogura, T. (2000a).

Zurzeit wird in Japan die technische Durchführbarkeit der Überwachung von Mobilkommunikation diskutiert. Die National Police Agency hat NTT Docomo aufgefordert, auf freiwilliger Basis ein System zu entwickeln, dass Überwachungsmaßnahmen ermöglicht. Dem Unternehmen ist es freigestellt, ob es der Aufforderung nachkommt, weil es nicht im Rahmen des Gesetzes dazu verpflichtet werden kann. Da mit der Entwicklung hohe Kosten verbunden sind, ist zurzeit offen, ob NTT Docomo sich dazu bereit erklärt.[157]

9.2.3 Organisatorische Anforderungen

Im Gesetz ist in Art. 12 festgelegt, dass während der Überwachungsmaßnahme eine dafür zuständige Person des TK-Unternehmens anwesend sein muss, um Datenmissbrauch zu verhindern. Diese Dritten dürfen nicht von der überwachten Telekommunikation Kenntnis erlangen. Die Anforderung wird von den TK-Unternehmen als zu aufwändig kritisiert. Da eine Maßnahme zwischen 24 Stunden und 30 Tagen andauern kann, haben die Unternehmen angekündigt, dass sie diese Forderung nicht erfüllen können und werden. Das Gesetz sieht in diesem Fall vor, dass ersatzweise ein Vertreter der jeweiligen Kommunalregierung anwesend sein muss.

Das zuständige Justizministerium sowie andere Behörden, die im Bereich der TK-Überwachung autorisiert sind (National Police Agency und Public Prosecutor's Office) sowie weitere haben mit den TK-Unternehmen in Arbeitsgruppen über die künftige Art der Zusammenarbeitsverpflichtungen diskutiert. Ein offizieller „Code of Practice" o.ä., in dem weitere organisatorische oder technische Anforderungen formuliert sind, wurde jedoch nicht erarbeitet.

9.2.4 Ausnahmen

Die Unternehmen können die Zusammenarbeit ablehnen, wenn dafür legitime Gründe vorliegen. Als berechtigter Grund gilt, wenn die Überwachungsmaßnahmen unverhältnismäßig aufwändig in organisatorischer oder technischer Hinsicht sind. Beispielsweise muss eine Überwachung nicht durchgeführt werden, wenn dazu die Implementierung eines neuen technischen Systems oder die Entwicklung einer neuen Software notwendig sind.

Das zuständige Justizministerium hat in einer Debatte im Diet[158] erklärt, dass von kleineren ISP geringere Kooperationsanstrengungen erwartet werden und, wenn diese betroffen sind, jeweils die Frage der Verhältnismäßigkeit geprüft werden muss. Das

---

157 Zu den Gründen vgl. auch Kap. 9.2.4 Ausnahmen.
158 Bezeichnung für das jap. Unterhaus („Reichstag").

Gesetz sieht jedoch keine zahlenmäßige Grenze vor (z.B. wie die TKÜV, die Ausnahmen nach der Anzahl der Teilnehmer zulässt).

Besonderheit

In Japan ist die Überwachung der Telekommunikation von Journalisten, Rechtsanwälten, Ärzten u.ä. Berufsgruppen nicht verboten.

9.2.5 Genehmigungsverfahren für Überwachungsvorkehrungen

Da von den TK-Anbietern und –Anlagebetreibern nach CI-Act, Art. 11 nur bestehende technische Einrichtungen für die Überwachung zur Verfügung gestellt werden müssen, sind solche Genehmigungsverfahren nicht erforderlich.

9.3 Voraussetzungen für die Überwachung

9.3.1 Fälle, in denen das Überwachen der TK angeordnet werden kann

Die Möglichkeit der Überwachung von Telekommunikation ist ausdrücklich auf die Aufdeckung der folgenden Straftaten beschränkt:

- Drogenhandel,
- illegaler Waffenhandel,
- organisierter Mord,
- Schleusen von illegalen Immigranten nach Japan.

9.3.2 Genehmigung einer Überwachungsmaßnahme

Die Überwachung erfolgt auf der Basis einer richterlichen Anordnung eines District Court Judges auf Antrag eines Staatsanwalts oder eines höherrangigen Kriminalpolizeibeamten.

Expertenaussagen zufolge ist eine Genehmigung in folgenden Fällen laut CI-Act möglich:

- es liegt eine schwere Straftat vor,
- zur Verübung der Straftat wurde elektronische Kommunikation eingesetzt,

- es ist schwierig, die Straftat mit anderen Mitteln aufzudecken,
- die Überwachungsmaßnahme ist genauestens spezifiziert.

9.3.3 Möglicher Zeitraum der Überwachung

Die Überwachung der Telekommunikation wird durch einen Richter für zehn Tage genehmigt, und kann auf maximal dreißig Tage erweitert werden.

9.3.4 Überprüfung der Rechtmäßigkeit der Maßnahme durch die Verpflichteten

Es ist keine solche Prüfung vorgesehen, da die Maßnahmen von den Strafverfolgungsbehörden selbst durchgeführt werden.

9.4 Durchführung der Überwachung

9.4.1 Erforderliche Angaben

Nach CI-Act, Art. 3 und 6 muss in der Anordnung der Name des Verdächtigen sowie die zu überwachenden Kennungen (Telefonnummer etc.) enthalten sein.

9.4.2 Art der zu überwachenden Telekommunikation

Zu Überwachen ist Telekommunikation während des Übertragungsprozesses in Echtzeit.

9.4.3 Übermittlung an die berechtigten Stellen

Es darf nur Echtzeit-Kommunikation überwacht werden. Dies geschieht in Anwesenheit eines Beamten der Strafverfolgungsbehörden an der technischen Einrichtung des TK-Anbieters bzw. -Anlagenbetreibers, so dass sich die Frage der Übermittlung in dieser Form nicht stellt.

9.4.4 Unterschiedliche technische Einrichtungen für verschiedene Überwachungsanforderungen

Die Unternehmen sind nur verpflichtet, die Strafverfolgungsbehörden bei der Durchführung von Maßnahmen zu unterstützen und innerhalb dieser Kooperation (ausschließlich) die bereits existierende technische Ausrüstung und Technologie zur Verfügung zu stellen (CI-Act, Art. 11).

9.4.5 Echtzeit-Überwachung oder Speicherung

Das TK-Überwachungsgesetz regelt nur Maßnahmen im Zusammenhang mit Echtzeit-Kommunikation (CI-Act, Art. 2). Die Ermittler müssen die Überwachung als „Spot Monitoring" durchführen.[159] Das bedeutet, dass nur Teile der Telekommunikation live überwacht werden dürfen. Geben diese Stichproben keinen Aufschluss über strafrechtlich relevante Handlungen, muss die Überwachung abgebrochen werden.

Die Überwachung von E-Mail erfolgt nicht nach dem CI-Act sondern nach den allgemeinen Befugnissen zu Durchsuchung und Beschlagnahmung. Es ist gängige Praxis, dass Server der ISP auf E-Mails von zu Überwachenden durchsucht werden.

Für E-Mails wird eine Speicher-Lösung namens „Temporary Mailbox" realisiert, die die Echtzeit-Überwachung von E-Mails vor Ort beim ISP ermöglicht. Die ISP müssen dazu eine Schnittstelle zur Verfügung stellen. Presseberichten zufolge sollen der Tokyo Metropolitan Police 2 und den 15 regionalen Polizeihauptquartieren jeweils eine technische Ausrüstung zur Verfügung stehen.[160]

9.5 Kontroll- und Sanktionsmaßnahmen

9.5.1 Kontrollinstanzen

Eine Kontrolle der Überwachungsmaßnahme soll dadurch gewährleistet sein, dass ein Mitarbeiter des jeweiligen Unternehmens bzw. ein Vertreter einer Kommunalbehörde während der Überwachung anwesend ist, während ein Beamter der berechtigten Behörden die Maßnahme durchführt.

---

159 Vgl. Gilmer, L. R. (2002), S. 899.
160 Vgl. Ogura, T. (2000b).

Besonderheit

Personen, deren Telekommunikation überwacht wurde, müssen davon innerhalb von 30 Tagen benachrichtigt werden, jedoch nur, wenn sie mit einer Straftat in Verbindung gebracht werden konnten. Nach dieser Benachrichtigung muss die gesamte Telekommunikation, die keine strafverfolgungsrelevanten Informationen enthält, vernichtet werden. Unbeteiligte Personen, deren Telekommunikation im Verlauf der Überwachung abgehört wurde, werden nicht benachrichtigt.

9.5.2 Berichtspflichten

Die durchführenden Beamten sind dazu angehalten, Protokolle über die Überwachungsmaßnahmen zu führen.

9.5.3 Statistiken

CI-Act, Art. 29, verpflichtet die Regierung dazu, dem Diet jedes Jahr eine Statistik über die erfolgten TK-Überwachungen vorzulegen.

Im Februar 2001, rund sechs Monate nach Verabschiedung des Gesetzes, berichtete das zuständige Justizministerium offiziell, dass noch keine einzige TK-Überwachungsmaßnahme im Rahmen des Gesetzes durchgeführt worden war. Insgesamt wurden dem japanischen Parlament für die Jahre 2000 und 2001 null Fälle von TK-Überwachung gemeldet.[161]

Im Jahr 2002 scheint eine Trendwende begonnen zu haben. Im März 2002 berichtete die japanische Presse über einen ersten Fall von Drogenhandel, der mit Hilfe einer zehntägigen Überwachungsmaßnahme aufgeklärt worden sei.[162]

Der geringe Einsatz des Instruments der TK-Überwachung ist in Japan vermutlich auch darauf zurückzuführen, dass die japanische Polizei weitreichende Befugnisse und Ermessenspielräume besitzt, wenn es um Durchsuchungen oder vorübergehende Festnahmen geht. Richterliche Anordnungen sind in vielen dieser Fälle nicht notwendig bzw. ohne größeren Aufwand zu erhalten.[163]

---

161 Zum Vergleich: In Japan leben rund 126,9 Mio. Menschen.
162 Vgl. The Japan Times, March 31, 2002 sowie The Asahi Shimbun, April 1, 2002.
163 Vgl. Gilmer, L. R. (2002), S. 915.

9.5.4 Sanktionen

Es sind hohe Strafen für den Fall vorgesehen, dass das Instrument der TK-Überwachung missbraucht wird.[164] Verstöße gegen das Fernmeldegeheimnis werden mit bis zu drei Jahren Gefängnis bzw. einer Geldstrafe von bis zu eine Mio. Yen (rd. 8.000 Euro) geahndet.[165] Das TK-Überwachungsgesetz sieht keine Strafen für den Fall vor, wenn TK-Anbieter und –Anlagenbetreiber die Kooperation mit den Strafverfolgungsbehörden verweigern.

9.6 Kosten

9.6.1 Bewertung des Aufwands durch die Verpflichteten

Der stärkste Protest in Japan gegen die Verabschiedung des CI-Act wurde von der Rechtsanwaltskammer, Journalisten, Gewerkschaften sowie Datenschutz-NGOs formuliert. Letztere besitzen jedoch in Japan einen weniger großen Einfluss als beispielsweise Gruppen in den USA.

Eine Auswertung der vorhandenen Sekundärliteratur enthält kaum Anhaltspunkte dafür, dass die Industrie öffentlich verstärkt gegen die Überwachungsanforderungen protestiert. Eine Ausnahme bildet die Regelung, wonach bei Überwachungsmaßnahmen ein Mitarbeiter des Unternehmens ständig zugegen sein muss. Diese Bestimmung erscheint den TK-Anbietern und –Anlagebetreibern zu kostenaufwändig. Es wird von Seiten der Behörden überlegt, dafür eine Entschädigung zu zahlen, es gibt dazu aber noch keine konkreten Überlegungen.

9.6.2 Kostenübernahme und Aufwandsentschädigungen

Ein Grund für den zurückhaltenden Protest der Unternehmen scheint zu sein, dass die Regierung einen Großteil der Kosten für die Entwicklung von Überwachungseinrichtungen zu tragen bereit ist. So forderte die National Police Agency zusammen mit dem Justizministerium von der Regierung die Bereitstellung von rund 170 Mio. Yen (1,37 Mio. Euro) für 2001, um die „Temporary Mailbox“ für das Aufzeichnen von E-Mail zu entwickeln.[166] Die Mailbox steht den regionalen Polizeibehörden zum Einsatz zur Verfügung, die sie dann fallweise installieren.

---

164 Vgl. EPIC/PI (Eds.) (2002), S. 237.
165 Vgl. die Angaben auf http://www.moj.go.jp/HOUAN/houan02.html.
166 Vgl. EPIC/PI (Eds.) (2002), S. 237.

Im Gesetz ist das Zahlen einer Aufwandsentschädigungen nicht vorgesehen. Es gab Debatten im Diet über das von den TK-Anbietern und -Anlagenbetreibern erwartete Ausmaß an Kooperation. Anlässlich dieser Diskussionen betonte das zuständige Justizministerium in einer Erklärung im Parlament ausdrücklich, dass unter der Voraussetzung, dass die Anforderungen die Ausstattung und die Technologie des Unternehmens überschreiten, oder sie die Geschäftstätigkeit gravierend stören, der TK-Anbieter bzw. -Anlagenbetreiber legitime Gründe hat, die Kooperation zu verweigern.

Literatur

Administrative Office of the United States Courts (AO) (2002): Report of the Director of the AO on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications, May 2002

AFA (o.J.): Pratiques et usages des Membres de l'AFA, Paris

Anti-terrorism, Crime and Security Act 2001, 2001 Chapter 24, Act of Parliament [United Kingdom]

Bäumler, H.; Leutheusser-Schnarrenberger, S.; Tinnefeld, M.-T. (2002): Grenzenlose Überwachung des Internets?, in: DuD 26 (2002), 9, S. 562

Bizer, Johann (2002): Telekommunikation und innere Sicherheit 2001. Neuere Entwicklungen im Telekommunikationsrecht, in: Kubicek, H. u.a. (Hrsg.), Innovation @ Infrastruktur, Jahrbuch Telekommunikation und Gesellschaft 2002, Heidelberg, S. 466-486

Bundesdatenschutzgesetz vom 18 Mai 2001, Bundesgesetzblatt I Nr. 23/2001, Seite 904, 22. Mai 2001

CNCIS (2002): 10e rapport d'activité 2001, Paris

CNCIS (o.J.): Commission nationale de contrôle des interceptions de sécurité – Die Nationale Kontrollkommission für sicherheitsbedingte Abhörmaßnahmen [Informationspapier der Kommission in deutscher Sprache], Paris

Commission of the European Communities (1998a): Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations, Official Journal L 204, 21.07.1998, pp. 37 - 48

Commission of the European Communities (1998b): Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations, Official Journal L 217, 05.08.1998, pp. 18 - 26

Council of Europe (2001): Convention on Cybercrime, ETS no. 185, Treaty open for signature by the member States and the non-member States which have participated in its elaboration and for accession by other non-member States

Decreto Legislativo 13 maggio 1998, n. 171 Disposizioni in materia di tutela della vita privata nel settore delle telecommunicazioni, in attuazione della direttiva 97/66/CE del Parlamento europeo e del Consiglio, ed in tema die attivata' giornalistica, pubblicato nella Gazzetta Uffizciale n 127 del 3 giugno 1998

Department of Justice; Industry Canada and Solicitor General (2002): Lawful Access – Consultation Document, Government of Canada, 25 August 2002

Department of the Solicitor General of Canada (2001): Annual Report on the Use of Electronic Surveillance 2000, Ottawa

Deutscher Bundestag (2002): Entwurf eines Gesetzes zur Verbesserung der Ermittlungsmaßnahmen wegen des Verdachts sexuellen Missbrauchs von Kindern und der Vollstreckung freiheitsentziehender Sanktionen, Gesetzentwurf des Bundesrates, BT-Drucksache 14/9801, 17.07.2002

Deutscher Bundestag (2002): Gesetzesentwurf des Bundesrates zur Verbesserung der Ermittlungsmaßnahmen wegen des Verdachts sexuellen Missbrauchs von Kindern und der Vollstreckung freiheitsentziehender Sanktionen, sowie Stellungnahme der Bundesregierung (Anlage 2), Drucksache 14/9801 v. 17.07.2002

DoJ / FBI (2001): Overview of CALEA, June 2001

DoJ, Criminal Devision, Computer Crime and Intellectual Property Section (2002): Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, July 2002

DoJ/OIG (2002): Implementation of the Communications Assistance For Law Enforcement Act by the Federal Bureau of Investigation, Report No. 02-14, March 2002

Elder, D. (2002): Telecommuncations Common Carriers and Subscriber Privacy: „Collateral Damage“ in the War on Terrorism?, Paper presented at the biannual Communications Law and Policy Conference of the Law Society of Upper Canada, Ottawa 2002

EPIC/PI (Eds.) (2002): Privacy and Human Rights 2002. An International Survey of Privacy Laws and Developments, Washington, London

ETSI (2001): Telecommunications Security; Lawful Interception (LI); Requirements of Law Enforcement Agencies, ETSI TS 101 331 V1.1.1 (2001-08) Technical Specification

EUROPOL (2001): List of minimum and optional data to be retained by service providers and Telcos, Questionnaire for Expert Meeting on Cyber Crime: Data Retention, The Hague, 28 December 2001, File 5121-20020411LR

FBI / DoJ (2001): Communications Assistance for Law Enforcement Act (CALEA), The Attorney General's Seventh Annual Report to Congress, December 17, 2001

General Secretatriat of the Council (2002): Presentation by the Presidency of answers to questionnaire on retention of traffic data, doc. 11490/1/02 CRIMORG 67 TELECOM 4 REV 1, Room Document No. 7, Multidisciplinary Group on Organised Crime, Brussels, 16 September 2002 [vertrauliches Dokument, im Internet verfügbar]

Gilmer, L. R. (2002): Japan's Communications Interception Act: Unconstitutional Invasion of Privacy or Necessary Tool?, in: Vanderbilt Journal of Transnational Law, Vol. 35, March 2002, No. 3, pp. 893-923

Home Office (Hrsg.) (2002): Interception of Communications. Code of Practice. Pursuant to Section 71 of the Regulation of Investigatory Powers Act 2000

Interception of Communications Commissioner (2000): Annual Report of the Interception of Communications Commissioner for 1999, London

Interception of Communications Commissioner (2001): Report of the Interception of Communications Commisioner for 2000, London, October 2001

Interception of Communications Commissioner (2002): Report of the Interception of Communications Commisioner for 2001, London, October 2002

Kirton, J.; Kokotsis, E. (2002): Keeping Genoa's Commitments: The 2002 G8 Research Group Compliance Report, University of Toronto, June 2002

Kommission der Europäischen Gemeinschaften (1995): Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Amtsblatt Nr. L 281 vom 23/11/1995 S. 31 – 50

Kommission der Europäischen Gemeinschaften (1997): Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation, Amtsblatt Nr. L 024 vom 30/01/1998 S. 1 - 8

Kommission der Europäischen Gemeinschaften (2000): Schaffung einer sichereren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität, Mitteilung der Kommission an den Rat, das Europäische Parlament, den Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, KOM(2000) 890 endg., 26. Januar 2001, Brüssel

Kommission der Europäischen Gemeinschaften (2001): Mitteilung der Kommission an den Rat, das europäische Parlament, den Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Schaffung einer sichereren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität (eEurope 2002), KOM(2000) 890endg. v. 26.01.2001, Brüssel

Kommission der Europäischen Gemeinschaften (2002): Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) Amtsblatt Nr. L 201 vom 31.07.2002, S. 37 - 47

Lücking, E. (1992): Die strafprozessuale Überwachung des Fernmeldeverkehrs. Eine rechtsvergleichende Untersuchung, Beiträge und Materialien aus dem Max-Planck-Institut für ausländisches und internationales Strafrecht, Freiburg

Ogura, T. (2000a): Toward Global Communication Rights: Movements against Wiretapping and Monitoring in Japan, 30. Oktober 2000,

Ogura, T. (2000b): New e-mail tapping device planned by law enforcement in Japan, 13. November 2000, http://cryptome.org/carnivore-jp.htm

Pallasky, A. (2002): USA PATRIOT Act: Neues Recht der TK-Überwachung, in: Datenschutz und Datensicherheit, 26 (2002) 4, S. 221 - 225

Privacy Commissioner of Canada (2002): Letter by George Radwanski, Privacy Commissioner of Canada to the Honourable Martin Cauchon, Minister of Justice and the Attorney General of Canada, the Honourable Wayne Easter, Solicitor General of Canada, and the Honourable Allan Rock, Minister of Industry, regarding the „Lawful Access“ proposals, 25. November 2002

Rat der Europäischen Union (1995): Entschließung des Rates vom 17. Januar 1995 über die rechtmäßige Überwachung des Fernmeldeverkehrs, Amtsblatt der Europäischen Gemeinschaften v. 4.11.96, Nr. C 329/1

Rat der Europäischen Union (2001): Entschließung über die operativen Anforderungen der Strafverfolgung in Bezug auf öffentliche Telekommunikationsnetze und –dienste, ENFOPOL 55, Brüssel, 20. Juni 2001

Security Intelligence Review Committee (2001): SIRC Report 2000-2001: An Operational Audit of the Canadian Security Intelligence Service, Ottawa

Surtees, L.; Chaisatien, W. (2002): Caught in the Web: Ottawa's Implementation of Cybercrime Treaty Requires Online Surveillance by xSPs, Canadian Telecom Market Drivers and Strategies Bulletin, IDC Canada, August 2002

TIA (2000): Interim Standard (Trial Use Standard) TIA/EIA/IS-J-STD-025-A, May 2000

Als "Diskussionsbeiträge" des Wissenschaftlichen Instituts für Kommunikationsdienste sind zuletzt erschienen:

Nr. 164: Hans Björn Rupp:

Ein Preissystem für das Internet, August 1996

Nr. 165: Alfons Keuter, Lorenz Nett, Ulrich Stumpf:

Regeln für das Verfahren zur Versteigerung von ERMES-Lizenzen/Frequenzen sowie regionaler ERMES-Frequenzen, September 1996

Nr. 166: Brigitte Bauer:

Nutzerorganisation und -repräsentation in der Telekommunikation, Oktober 1996

Nr. 167: Franz Büllingen unter Mitarbeit von Frank Stöckler:

Die Entwicklung des Seniorenmarktes und seine Bedeutung für den Telekommunikationssektor, November 1996

Nr. 168: Ingo Vogelsang:

Wettbewerb im Ortsnetz - Neue Entwicklungen in den USA, Dezember 1996

Nr. 169: Marta Garcia Arranz, Klaus D. Hackbarth unter Mitarbeit von Bernd Ickenroth:

Kosten von vermittelten Leitungen in digitalen Netzen, Dezember 1996

Nr. 170: Monika Plum, Stephan Steinmeyer:

Preisdifferenzierung im Briefdienst - volkswirtschaftliche und unternehmenspolitische Aspekte, Februar 1997

Nr. 171: Daniel Tewes:

Entwicklungsstand und Märkte funkgestützter Ortsnetztechnologien, März 1997

Nr. 172: Peter Kürble:

Branchenstrukturanalyse im Multimedia-Markt am Beispiel der Spielfilmbranche und der Branche der Programmveranstalter, April 1997

Nr. 173: Federico Kuhlmann:

Entwicklungen im Telekommunikationssektor in Mexiko: Von einem Staatsmonopol zum Wettbewerb, April 1997

Nr. 174: Jörn Kruse:

Frequenzvergabe im digitalen zellularen Mobilfunk in der Bundesrepublik Deutschland, Mai 1997

Nr. 175: Annette Hillebrand, Franz Büllingen, Olaf Dickoph, Carsten Klinge:

Informations- und Telekommunikationssicherheit in kleinen und mittleren Unternehmen, Juni 1997

Nr. 176: Wolfgang Elsenbast:

Ausschreibung defizitärer Universaldienste im Postbereich, August 1997

Nr. 177: Uwe Rabe:

Konzeptionelle und operative Fragen von Zustellnetzen, November 1997

Nr. 178: Dieter Elixmann, Alfons Keuter, Bernd Meyer:

Beschäftigungseffekte von Privatisierung und Liberalisierung im Telekommunikationsmarkt, November 1997

Nr. 179: Daniel Tewes:

Chancen und Risiken netzunabhängiger Service Provider, Dezember 1997

Nr. 180: Cara Schwarz-Schilling:

Nummernverwaltung bei Wettbewerb in der Telekommunikation, Dezember 1997

also available in English as Numbering Administration in Telecommunications under Competitive Conditions

Nr. 181: Cornelia Fries:

Nutzerkompetenz als Determinante der Diffusion multimedialer Dienste, Dezember 1997

Nr. 182: Annette Hillebrand:

Sicherheit im Internet zwischen Selbstorganisation und Regulierung - Eine Analyse unter Berücksichtigung von Ergebnissen einer Online-Umfrage, Dezember 1997

Nr. 183: Lorenz Nett:

Tarifpolitik bei Wettbewerb im Markt für Sprachtelefondienst, März 1998

Nr. 184: Alwin Mahler:

Strukturwandel im Bankensektor - Der Einfluß neuer Telekommunikationsdienste, März 1998

Nr. 185: Henrik Hermann:

Wettbewerbsstrategien alternativer Telekommunikationsunternehmen in Deutschland, Mai 1998

Nr. 186: Ulrich Stumpf, Daniel Tewes:

Digitaler Rundfunk - vergleichende Betrachtung der Situation und Strategie in verschiedenen Ländern, Juli 1998

Nr. 187: Lorenz Nett, Werner Neu:

Bestimmung der Kosten des Universaldienstes, August 1998

Nr. 188: Annette Hillebrand, Franz Büllingen:

Durch Sicherungsinfrastruktur zur Vertrauenskultur: Kritische Erfolgsfaktoren und regulatorische Aspekte der digitalen Signatur, Oktober 1998

Nr. 189: Cornelia Fries, Franz Büllingen:

Offener Zugang privater Nutzer zum Internet - Konzepte und regulatorische Implikationen unter Berücksichtigung ausländischer Erfahrungen, November 1998

Nr. 190: Rudolf Pospischil:

Repositionierung von AT&T - Eine Analyse zur Entwicklung von 1983 bis 1998, Dezember 1998

Nr. 191: Alfons Keuter:

Beschäftigungseffekte neuer TK-Infrastrukturen und -Dienste, Januar 1999

Nr. 192: Wolfgang Elsenbast:

Produktivitätserfassung in der Price-Cap-Regulierung – Perspektiven für die Preisregulierung der Deutschen Post AG, März 1999

Nr. 193: Werner Neu, Ulrich Stumpf, Alfons Keuter, Lorenz Nett, Cara Schwarz-Schilling:

Ergebnisse und Perspektiven der Telekommunikationsliberalisierung in ausgewählten Ländern, April 1999

Nr. 194: Ludwig Gramlich:

Gesetzliche Exklusivlizenz, Universaldienstpflichten und "höherwertige" Dienstleistungen im PostG 1997, September 1999

Nr. 195: Hasan Alkas:

Rabattstrategien marktbeherrschender Unternehmen im Telekommunikationsbereich, Oktober 1999

Nr. 196: Martin Distelkamp:

Möglichkeiten des Wettbewerbs im Orts- und Anschlußbereich des Telekommunikationsnetzes, Oktober 1999

Nr. 197: Ulrich Stumpf, Cara Schwarz-Schilling unter Mitarbeit von Wolfgang Kiesewetter:

Wettbewerb auf Telekommunikationsmärkten, November 1999

Nr. 198: Peter Stamm, Franz Büllingen:

Das Internet als Treiber konvergenter Entwicklungen – Relevanz und Perspektiven für die strategische Positionierung der TIME-Player, Dezember 1999

Nr. 199: Cara Schwarz-Schilling, Ulrich Stumpf:

Netzbetreiberportabilität im Mobilfunkmarkt – Auswirkungen auf Wettbewerb und Verbraucherinteressen, Dezember 1999

Nr. 200: Monika Plum, Cara Schwarz-Schilling:

Marktabgrenzung im Telekommunikations- und Postsektor, Februar 2000

Nr. 201: Peter Stamm:

Entwicklungsstand und Perspektiven von Powerline Communication, Februar 2000

Nr. 202: Martin Distelkamp, Dieter Elixmann, Christian Lutz, Bernd Meyer, Ulrike Schimmel:

Beschäftigungswirkungen der Liberalisierung im Telekommunikationssektor in der Bundesrepublik Deutschland, März 2000

Nr. 203: Martin Distelkamp:

Wettbewerbspotenziale der deutschen Kabel-TV-Infrastruktur, Mai 2000

Nr. 204: Wolfgang Elsenbast, Hilke Smit:

Gesamtwirtschaftliche Auswirkungen der Marktöffnung auf dem deutschen Postmarkt, Mai 2000

Nr. 205: Hilke Smit:

Die Anwendung der GATS-Prinzipien auf dem Postsektor und Auswirkungen auf die nationale Regulierung, Juni 2000

Nr. 206: Gabriele Kulenkampff:

Der Markt für Internet Telefonie - Rahmenbedingungen, Unternehmensstrategien und Marktentwicklung, Juni 2000

Nr. 207: Ulrike Schimmel:

Ergebnisse und Perspektiven der Telekommunikationsliberalisierung in Australien, August 2000

Nr. 208: Franz Büllingen, Martin Wörter:

Entwicklungsperspektiven, Unternehmensstrategien und Anwendungsfelder im Mobile Commerce, November 2000

Nr. 209: Wolfgang Kiesewetter:

Wettbewerb auf dem britischen Mobilfunkmarkt, November 2000

Nr. 210: Hasan Alkas:

Entwicklungen und regulierungspolitische Auswirkungen der Fix-Mobil Integration, Dezember 2000

Nr. 211: Annette Hillebrand:

Zwischen Rundfunk und Telekommunikation: Entwicklungsperspektiven und regulatorische Implikationen von Webcasting, Dezember 2000

Nr. 212: Hilke Smit:

Regulierung und Wettbewerbsentwicklung auf dem neuseeländischen Postmarkt, Dezember 2000

Nr. 213: Lorenz Nett:

Das Problem unvollständiger Information für eine effiziente Regulierung, Januar 2001

Nr. 214: Sonia Strube:

Der digitale Rundfunk - Stand der Einführung und regulatorische Problemfelder bei der Rundfunkübertragung, Januar 2001

Nr. 215: Astrid Höckels:

Alternative Formen des entbündelten Zugangs zur Teilnehmeranschlussleitung, Januar 2001

Nr. 216: Dieter Elixmann, Gabriele Kulenkampff, Ulrike Schimmel, Rolf Schwab:

Internationaler Vergleich der TK-Märkte in ausgewählten Ländern - ein Liberalisierungs-, Wettbewerbs- und Wachstumsindex, Februar 2001

Nr. 217: Ingo Vogelsang:

Die räumliche Preisdifferenzierung im Sprachtelefondienst - wettbewerbs- und regulierungspolitische Implikationen, Februar 2001

Nr. 218: Annette Hillebrand, Franz Büllingen:

Internet-Governance - Politiken und Folgen der institutionellen Neuordnung der Domainverwaltung durch ICANN, April 2001

Nr. 219: Hasan Alkas:

Preisbündelung auf Telekommunikationsmärkten aus regulierungsökonomischer Sicht, April 2001

Nr. 220: Dieter Elixmann, Martin Wörter:

Strategien der Internationalisierung im Telekommunikationsmarkt, Mai 2001

Nr. 221: Dieter Elixmann, Anette Metzler:

Marktstruktur und Wettbewerb auf dem Markt für Internet-Zugangsdienste, Juni 2001

Nr. 222: Franz Büllingen, Peter Stamm:

Mobiles Internet - Konvergenz von Mobilfunk und Multimedia, Juni 2001

Nr. 223: Lorenz Nett:

Marktorientierte Allokationsverfahren bei Nummern, Juli 2001

Nr. 224: Dieter Elixmann:

Der Markt für Übertragungskapazität in Nordamerika und Europa, Juli 2001

Nr. 225: Antonia Niederprüm:

Quersubventionierung und Wettbewerb im Postmarkt, Juli 2001

Nr. 226: Ingo Vogelsang
unter Mitarbeit von Ralph-Georg Wöhrl

Ermittlung der Zusammenschaltungsentgelte auf Basis der in Anspruch genommenen Netzkapazität, August 2001

Nr. 227: Dieter Elixmann, Ulrike Schimmel, Rolf Schwab:

Liberalisierung, Wettbewerb und Wachstum auf europäischen TK-Märkten, Oktober 2001

Nr. 228: Astrid Höckels:

Internationaler Vergleich der Wettbewerbsentwicklung im Local Loop, Dezember 2001

Nr. 229: Anette Metzler:

Preispolitik und Möglichkeiten der Umsatzgenerierung von Internet Service Providern, Dezember 2001

Nr. 230: Karl-Heinz Neumann:

Volkswirtschaftliche Bedeutung von Resale, Januar 2002

Nr. 231: Ingo Vogelsang:

Theorie und Praxis des Resale-Prinzips in der amerikanischen Telekommunikationsregulierung, Januar 2002

Nr. 232: Ulrich Stumpf:

Prospects for Improving Competition in Mobile Roaming, März 2002

Nr. 233: Wolfgang Kiesewetter:

Mobile Virtual Network Operators – Ökonomische Perspektiven und regulatorische Probleme, März 2002

Nr. 234: Hasan Alkas:

Die Neue Investitionstheorie der Realoptionen und ihre Auswirkungen auf die Regulierung im Telekommunikationssektor, März 2002

Nr. 235: Karl-Heinz Neumann:

Resale im deutschen Festnetz, Mai 2002

Nr. 236: Wolfgang Kiesewetter, Lorenz Nett und Ulrich Stumpf:

Regulierung und Wettbewerb auf europäischen Mobilfunkmärkten, Juni 2002

Nr. 237: Hilke Smit:

Auswirkungen des e-Commerce auf den Postmarkt, Juni 2002

Nr. 238: Hilke Smit:

Reform des UPU-Endvergütungssystems in sich wandelnden Postmärkten, Juni 2002

Nr. 239: Peter Stamm, Franz Büllingen:

Kabelfernsehen im Wettbewerb der Plattformen für Rundfunkübertragung - Eine Abschätzung der Substitutionspotenziale, November 2002

Nr. 240: Dieter Elixmann, Cornelia Stappen
unter Mitarbeit von Anette Metzler:

Regulierungs- und wettbewerbspolitische Aspekte von Billing- und Abrechnungsprozessen im Festnetz, Januar 2003

Nr. 241: Lorenz Nett, Ulrich Stumpf
unter Mitarbeit von Ulrich Ellinghaus, Joachim Scherer, Sonia Strube Martins, Ingo Vogelsang:

Eckpunkte zur Ausgestaltung eines möglichen Handels mit Frequenzen, Februar 2003

Nr. 242: Christin-Isabel Gries:

Die Entwicklung der Nachfrage nach breitbandigem Internet-Zugang, April 2003

Nr. 243: Wolfgang Briglauer:

Generisches Referenzmodell für die Analyse relevanter Kommunikationsmärkte – Wettbewerbsökonomische Grundfragen, Mai 2003

Nr. 244: Peter Stamm, Martin Wörter:

Mobile Portale – Merkmale, Marktstruktur und Unternehmensstrategien, Juli 2003

Nr. 245: Franz Büllingen, Annette Hillebrand:

Sicherstellung der Überwachbarkeit der Telekommunikation: Ein Vergleich der Regelungen in den G7-Staaten, Juli 2003