Hochschule für Telekommunikation, Leipzig

Aspekte des ICT-Rechts

Sebastian Lammermann

Hochschule für Telekommunikation, Leipzig

Aspekte des ICT-Rechts

Seminararbeit

Verfasser:	Sebastian Lammermann
	Matrikelnummer 074111
Betreuerin:	Prof. Dr.-Ing. S. Wieland
Fertigstellung:	29. Januar 2009
Kontakt:	sebastian@lammermann.eu

Inhalt

1 Vorwort, Abgrenzung und Hinweise **1**

2 Einleitung **1**

3 Onlinedurchsuchung **2**

3.1 Motivation *2*

3.2 Gesetzeslage *3*

3.3 Rechtsprechung *4*

3.4 Technische Umsetzung *5*

3.5 Fazit *7*

4 Vorratsdatenspeicherung **8**

4.1 Motivation *8*

4.2 Gesetzeslage *9*

4.3 Rechtsprechung *11*

4.4 Technische Umsetzung *12*

4.5 Fazit *13*

5 Rechtliches zu WLANs **15**

5.1 Motivation *15*

5.2 Gesetzeslage zum „Schwarzsurfen“ *16*

5.3 Rechtsprechung zum „Schwarzsurfen“ *16*

5.4 Technische Aspekte zum „Schwarzsurfen“ *17*

5.5 Gesetzeslage zur Störerhaftung *18*

5.6 Rechtsprechung zur Störerhaftung *19*

5.7 Technische Aspekte zur Störerhaftung *20*

5.8 Fazit *21*

6 Zusammenfassung **22**

1 Vorwort, Abgrenzung und Hinweise

Die vorliegende Seminararbeit zum Thema *Aspekte des ICT-Rechts* entstand im Rahmen des Lehrgebiets „Verteilte Systeme“ im Wintersemester 2008/2009 an der Hochschule für Telekommunikation, Leipzig.

Abkürzungen werden in dieser Projektarbeit in der Regel mit Artikel, sowie ggf. mit Genitiv-s versehen. Um einen besseren Lesefluss zu ermöglichen, wird eine eingeführte Abbreviatur nicht durchgehend verwendet, sondern stellenweise die ausgeschriebene Variante bevorzugt.

Im vorliegenden Text wird sowohl für die Transkription als auch für die Translation des griechischen Buchstabens 'Φ', außer bei Namen, ausschließlich die offizielle neugriechische Übersetzung 'F' verwendet. Damit wird die Schreibweise des Dudens in einigen Fällen missachtet. Da dieser allerdings 1998 seine Monopolstellung bei der Rechtschreibung verloren hat und nun vielmehr Richtlinien beinhaltet, sei hiermit auf diese Hinwegsetzung aufmerksam gemacht.

In dieser Arbeit wird ausschließlich die Rechtslage in der Bundesrepublik Deutschland beschrieben.

2 Einleitung

Ziel dieser Seminararbeit ist es, vier Aspekte der für die *Informations- und Kommunikationstechnik* (*information and communication technology*, *ICT*) relevanten Rechtslage vorzustellen. Gewählt wurden Themen, die allesamt von aktueller Bedeutung sind:

- **Kapitel 3** beschäftigt sich mit der Onlinedurchsuchung
- **Kapitel 4** beleuchtet die Vorratsdatenspeicherung
- **Kapitel 5** betrachtet zwei für Funknetzwerke relevante rechtliche Aspekte: das „Schwarzsurfen“ über einen fremden Internetanschluss und die Störerhaftung bei Missbrauch
- Darüber hinaus bietet **Kapitel 6** eine Zusammenfassung dieser Arbeit

Jedes der Hauptkapitel ist in mehrere Abschnitte unterteilt:

- Die **Motivation** beschreibt, warum das Thema gewählt worden ist und verweist auf weitere Literatur
- Der Abschnitt zur **Gesetzeslage** beschreibt die aktuelle Rechtslage in der Bundesrepublik Deutschland, sowie ggf. deren Entwicklung

- Im Teil zur **Rechtsprechung** werden Gerichtsurteile wiedergegeben und erläutert
- Ferner wird die **technische Umsetzung** der jeweiligen Gesetze betrachtet und ggf. auf Schwierigkeiten bei der Realisierung hingewiesen
- In einem **Fazit** wird der Inhalt des jeweiligen Kapitels zusammengefasst und Stellung zum Thema bezogen

3 Onlinedurchsuchung

3.1 Motivation

Spätestens seit den Terroranschlägen vom 11. September 2001 ist ein internationaler Trend hin zu mehr Überwachung der eigenen Bevölkerung zu erkennen. Zunehmend wurden und werden Freiheiten zugunsten einer Law-and-Ordner-Politik eingeschränkt, ein kollektives Gefühl der Bedrohung durch terroristische Aktivitäten geschaffen und bewahrt. Geheimdienste[1] und Polizeien[2] werden zunehmend gestärkt.

Gleichzeitig ist seit einigen Monaten aber auch eine erstarkende Gegenbewegung erkennbar. Freiheitsrechte werden wieder intensiver in der Öffentlichkeit diskutiert, entsprechende Organisationen treten deutlich sichtbar auf den Plan und auch in der Politik setzen sich die Oppositionsparteien[3] allesamt für mehr BürgerInnenrechte ein. Nicht zuletzt dadurch werden weite Teile der Bevölkerung angesprochen.

In diesem Kontext erscheint die Debatte um die Onlinedurchsuchung zu einem sehr interessanten Zeitpunkt. Auf der einen Seite drängt die Bundesregierung und insbesondere das Innenministerium darauf, informationstechnische Systeme intensiver Überwachen zu können. Auf der andere Seite steht das wachsende Bewusstsein in der Bevölkerung, dass mit der zunehmenden Technisierung und Vernetzung des Alltags auch eine Art „digitales Leben“ entstanden ist, das einem besonderen Schutz bedarf.

Analog zu den anderen Teilen dieser Seminararbeit beschäftigt sich dieses Kapitel zuerst mit der aktuellen Gesetzeslage und beleuchtet dann die Rechtsprechung genauer. Daran anknüpfend werden Szenarien der technischen Realisierung analysiert und schließlich

1 In der Bundesrepublik Deutschland existieren zu diesem Zeitpunkt (29. Januar 2009) drei Geheimdienste des Bundes (Bundesnachrichtendienst, Bundesamt für den Verfassungsschutz, Militärischer Abschirmdienst), sowie sechzehn Geheimdienste der Länder (Landesamt für den Verfassungsschutz).

2 In der Bundesrepublik Deutschland existieren zu diesem Zeitpunkt (29. Januar 2009) sechzehn Polizeien der Länder, sowie die Bundespolizei, das Bundeskriminalamt und die Polizei beim Deutschen Bundestag.

3 Zu diesem Zeitpunkt (29. Januar 2009) wird die Bundesrepublik von einer „Großen Koalition“ regiert, bestehend aus konservativer CDU/CSU und sozialdemokratischer SPD. Die Oppositionsparteien sind die sozialistische Die Linke, die linksliberalen Bündnis 90/Die Grünen und die liberale FDP.

bewertet.

An Quellen sind als Einstieg in die Thematik besonders drei Folgen des Chaosradios zu empfehlen [CR_122][CR_127][CR_132], sowie das Buch „Die Online-Durchsuchung“ [ScSc08].

3.2 Gesetzeslage

Als so genannte „*Onlinedurchsuchung*“ oder „*Onlineüberwachung*“ wird eine Maßnahme bezeichnet, bei der auf einem entfernten Computer gespeicherte Daten ausgelesen werden, die für ein Ermittlungsverfahren relevant sein könnten [CR_122]. Sie ist damit beispielsweise von der sog. „*Quellentelekommunikationsüberwachung*“ (*Quellen-TKÜ*) zu unterscheiden, bei der zwar ein Telekommunikationsvorgang überwacht wird, die auf den Geräten gespeicherten Daten jedoch unberührt bleiben [§TKÜ07]. Der Mehrwert der Onlinedurchsuchung gegenüber einer Beschlagnahme von informationstechnischen Systemen[4] liegt in der Überwachung der Aktivitäten über einen längeren Zeitraum ohne Kenntnis der Betroffenen.

In der Bundesrepublik Deutschland sind geheimdienstliche Onlinedurchsuchungen seit 2005 öffentlich bekannt. Der damalige Bundesinnenminister Otto Schily unterzeichnete eine entsprechende Dienstvorschrift, die dem Bundesverfassungsschutz[5] die Möglichkeit gab, heimlich die Computersysteme von verdächtigen Personen auszuspionieren [Ster07].

Zusätzlich zur Bundesebene ermöglichen teilweise auch die Länder ihren Polizeien[6] oder ihrem jeweiligen Nachrichtendienst Onlinedurchsuchungen. So ist es z. B. dem Verfassungsschutz des Landes Nordrhein-Westfalen seit Ende 2006 gestattet, sich heimlich Zugriff auf informationstechnische Systeme zu verschaffen [§VSG06]. Im Freistaat Bayern verfügt außerdem die Polizei seit Juli 2008 ebenfalls über diese Befugnisse [§PAG08].

Nach dem Urteil des *Bundesverfassungsgerichts* (*BVerfG*) vom 27. Februar 2008 ist eine Onlinedurchsuchung „verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen“ [BVG108], also lediglich in Einzelfällen. Außerdem muss zuerst eine Ermächtigungsgrundlage geschaffen werden, bevor eine Onlinedurchsuchung überhaupt rechtmäßig sein kann. Das bedeutet, dass von der jeweiligen Regierung ein Gesetz erlassen werden muss, um Polizei bzw. Verfassungs-

4 Zu den informationstechnischen Systemen zählen z. B. Computer, Telekommunikationsgeräte, Rechnernetzwerke (u. a. das Internet), aber auch elektronische Geräte in Gebäuden und Fahrzeugen sowie elektronische Terminkalender.

5 Aufgabe des Bundesverfassungsschutz sowie der Verfassungsschutzbehörden der Länder sind z. B. die Spionageabwehr, die Abwehr von gegen die freiheitlich-demokratische Grundordnung gerichteten Bestrebungen und die Informationsbeschaffung [§AdV94].

6 Aufgaben der Polizeien sind die Abwehr von Gefahren sowie die Bekämpfung von Störungen der öffentlichen Sicherheit und Ordnung.

schutz die Durchsuchung von entfernten Computersystemen zu ermöglichen.

In der aktuellen Neufassung des „BKA-Gesetzes“ vom 25. Dezember 2008 ist u. a. der verdeckte Eingriff in informationstechnische Systeme vorgesehen [§BKA08]. Unter bestimmten Voraussetzungen – wie der Gefahr für Leib, Leben oder die Freiheit einer Person – ist es dem *Bundeskriminalamt* (*BKA*) gestattet in ein Computersystem einzudringen und aus diesem Daten zu erheben, sofern auf Antrag des BKA-Präsidenten oder seines Vertreters eine richterliche Anordnung ergeht. Eine Onlinedurchsuchung darf die Dauer von drei Monaten nicht überschreiten, auf richterliche Anordnung allerdings beliebig oft um jeweils weitere drei Monate verlängert werden. Es dürfen nur Daten erhoben werden, die für die Maßnahme relevant sind. Sofern einzig Erkenntnisse aus dem Privatleben gewonnen werden können, ist die Onlinedurchsuchung unzulässig. Grundsätzlich sind alle Änderungen am System nach Abschluss der Operation rückgängig zu machen.

Nach Presseberichten verfügen die Geheimdienste ebenfalls über Rechtsgrundlagen, um Onlinedurchsuchungen durchführen zu dürfen [Heis07].

3.3 Rechtsprechung

Ende 2006 stellte die Generalbundesanwaltschaft einen Antrag für eine Onlinedurchsuchung auf der Grundlage der Vorschriften zur Wohnungsdurchsuchung. Am 31. Januar 2007 fällte der *Bundesgerichtshof* (*BGH*) das abschließende Urteil. Demnach ist die bisherige Onlinedurchsuchung nicht mit dem geltenden Recht vereinbar und damit unzulässig. Dies betraf zunächst insbesondere die nordrhein-westfälische Regelung, die folglich nicht mehr verfassungskonform war. Der BGH bemerkte, dass das Durchforsten eines Datenträgers einer Durchsuchung im strafrechtlichen Sinn entspricht, dass imaginär vorliegende Informationen[7] als Beweismittel dienen können und dass EDV-Anlagen nicht grundsätzlich vom Zugriff der Behörden entzogen sind. Er stellt jedoch auch fest, dass eine geheime Onlinedurchsuchung die Betroffenen stärker belastet als eine klassische Wohnungsdurchsuchung, da die Durchsuchung weder abgewendet noch einen Rechtsbeistand hinzugezogen werden kann.

Seit dem Urteil gilt, dass eine Onlinedurchsuchung zwar zulässig sein kann, allerdings nur unter bestimmten Bedingungen [BVG108]. Außerdem wird vorausgesetzt, dass sowohl ein Gesetz besteht, dass dem entsprechenden Organ die Maßnahme gestattet und dass eine richterliche Anordnung zum Einzelfall vorliegt. Ferner dürfen nur für das Verfahren relevante Daten

7 Auf informationstechnischen Systemen gespeicherte Informationen liegen nicht in materieller Form vor. Sie sind als im Grunde imaginäre Daten anzusehen, die auf einem Medium (z. B. einer Festplatte) abgelegt sind und nur durch das System selbst interpretierbar werden.

erhoben werden, sonst ist die Überwachung unzulässig.

Mit dem Urteil des BVerfGs wurde darüber hinaus ein neues Grundrecht geschaffen: Das „*Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*“ (kurz: „*Grundrecht auf digitale Intimsfäre*“ [CR_132]). Durch dieses besteht seit der Urteilsverkündung einer besonderer Schutz von persönlichen Daten, die in informationstechnischen Systemen sowohl gespeichert als auch verarbeitet werden [Hoer08]. Es ist in der Verfassung nicht separat formuliert, sondern gilt aus Ausprägung des im zweiten Artikel des Grundgesetzes verankerten allgemeinen Persönlichkeitsrechts. Außer in den oben beschriebenen Ausnahmen ist das Ausspähen eines fremden Computersystems demnach ein Eindringen in die Intimsfäre einer Person und folglich unzulässig.

3.4 Technische Umsetzung

Wie eine Onlinedurchsuchung technisch realisiert wird, ist bisher noch nicht bekannt. In den Medien kursieren oftmals diverse Lösungen, bei denen die Zielperson aktiv eine so genannte „*Remote Forensic Software*“ (*RFS*)[8] auf ihrem Computer installieren muss [ScSc08][CR_127]. Ein entsprechendes Szenario wird oftmals wie folgt beschrieben: Die Zielperson erhält die RFS in Anhang einer als Werbe- oder Behörden-E-Mail getarnten Nachricht. Der Inhalt des Textes ist so gestaltet, dass die zu überwachende Person mit großer Wahrscheinlichkeit den Anhang öffnet und somit ein Programm ausführt, welches die RFS auf dem Zielcomputer installiert. In der Praxis wird dieses Vorgehen allerdings meist am Misstrauen der Zielperson scheitern, da insbesondere Behörden niemals E-Mails – also unverschlüsselte elektronische Postkarten[9] – versenden würden, sondern üblicherweise auf dem klassischen Postweg Kontakt aufnehmen. Wird versucht die RFS via Werbe-E-Mail zu versenden, könnte darüber hinaus schon der Spamfilter des E-Mail-Providers jeglichen Erfolg verhindern.

Theoretisch bestünde auch die Möglichkeit, eine RFS in Updates anderer Programme zu verstecken. Hierfür wäre es aber notwendig, die Verbindung über einen Proxyserver zu leiten, welcher die Pakete verändert und mit dem entsprechenden Spähprogramm versieht. Da in der Regel jedoch alle Updates mit einer Prüfsumme versehen sind, wird das System normalerweise die Installation verhindern, da die Pakete als fehlerhaft eingestuft würden. Außerdem setzt diese Methode voraus, dass die Zielperson überhaupt automatische Aktualisierungen

8 Engl.: „fernforensische Software“.

9 Eine unverschlüsselte und dazu noch unverschlüsselt übertragene E-Mail hat den Charakter einer Postkarte, da bei der Übermittlung die enthaltene Nachricht für alle Sichtbar ist, die die entsprechenden Datenpakete übertragen.

vornimmt.

Als dritte Vorgehensweise, um eine RFS auf einem Computer zu installieren, wird gelegentlich eine manipulierte Website aufgeführt. Hierbei soll die Zielperson zum Besuch einer bestimmten Seite im Internet gebracht werden, auf der dann z. B. ein Java Applet die Software auf der Festplatte installiert. Diese Vorgehensweise ist allerdings unrealistisch, selbst wenn ein Proxyserver den gesamten Verkehr auf manipulierte Kopien der zu besuchenden Websites umleiten würde. Denn es wird vorausgesetzt, dass einerseits Java o. ä. bereits auf dem Zielrechner installiert ist und andererseits der verwendete Browser die Ausführung von Scripten zulässt.

Sofern von der Zielperson ein schlecht gesichertes Funknetzwerk (*Wireless Local Area Network, WLAN*) betrieben wird, bestünde ferner die Möglichkeit, über jenes Zugriff auf das Computersystem zu erhalten. Um dies zu ermöglichen, muss allerdings einerseits der Zugang zum Zielrechner relativ schlecht geschützt sein (WLAN-Verschlüsselung, Netzwerksicherheit) und andererseits eine Sendestation in Empfangsreichweite des WLANs positioniert werden. Realisierbar wäre bei letzterem die Unterbringung des Senders im Hausflur, in einer Nachbarwohnung, oder – falls die Signalstärke dies zulässt – in einem Fahrzeug auf der Straße.

Denkbar ist auch, die RFS auf einer CD oder einem anderen Datenträger zu speichern. Dieses Medium würde der betroffenen Person per Post o. ä. zugestellt und ist so gestaltet, dass es mit hoher Wahrscheinlichkeit mit dem Zielsystem verbunden wird und es zu einer Installation der Überwachungssoftware käme. Auch hier wird auf die „Sicherheitslücke Mensch“ gesetzt, also davon ausgegangen, dass keinerlei Misstrauen gegenüber eines solchen Datenträgers besteht.

Die einzige Methode mit der die Installation auf einem Computer mit relativ hoher Wahrscheinlichkeit gelingt, ist der fysikalische Zugriff auf das Gerät. Hierfür ist mindestens das einmalige Eindringen in die Wohnung der Zielperson nötig, um die Remote Forensic Software auf dem System vor Ort zu installieren. Rechtlich ist dies allerdings nicht zulässig, da dies nicht mit der Verfassung vereinbar wäre[10]. Unabhängig davon wird auch hier vorausgesetzt, dass das Zielsystem relativ unsicher ist und beispielsweise nicht durch Passwörter und/oder eine Festplattenverschlüsselung geschützt wird.

Ist die RFS einmal installiert, könnte es dann, je nach Funktionsumfang des Programms, möglich sein, das System komplett aus der Ferne zu überwachen und ggf. auch zu steuern. Sinn macht diese Vorgehensweise allerdings nur, wenn die betroffene Person nicht über die

10 Art. 13 GG: Unverletzlichkeit der Wohnung. Jede polizeiliche oder geheimdienstliche Maßnahme, bei der in den Wohnraum eingedrungen werden muss, hat offen stattzufinden. Die Betroffenen müssen folglich informiert werden und es muss für sie die Möglichkeit bestehen, einen Rechtsbeistand hinzuzuziehen.

Überwachungsmaßnahme informiert wird.

3.5 Fazit

In einer Zeit, in der wir uns mehr und mehr zu einer digitalen Informationsgesellschaft entwickeln, ist es unerlässlich, auch dem Staat die Möglichkeit zu geben, computergestützte Kriminalität zu bekämpfen. Auf den ersten Blick mag es darum wie selbstverständlich erscheinen, dass Polizeien und Geheimdienste unter bestimmten Umständen private Computer über das Internet nach verdächtigen Dateien ausspähen dürfen.

Dabei wird allerdings oftmals vergessen, dass staatliche Organe auch nach der bisher geltenden Gesetzeslage weit reichende Möglichkeiten haben, um die Systeme verdächtiger Personen zu untersuchen. Da z. B. nicht nur klassische Telefonie, sondern auch die computergestützte Verständigung über das Internet als Telekommunikation gilt, darf auch diese überwacht werden. Dies gibt zwar nicht in erster Linie Aufschluss über die auf dem Rechner gespeicherten Daten, hat dafür aber zwei entscheidende Vorteile: Wenn eine verdächtige Person schon das Internet mit einem Rechner nutzt, auf dem sich ermittlungsrelevante Daten befinden, so werden diese Inhalte mit Sicherheit auch irgendwann über das Internet übertragen. Sie können folglich mit einer relativ hohen Wahrscheinlichkeit auch auf diesem Weg erhoben werden. Darüber hinaus ermöglicht die Telekommunikationsüberwachung einzig den Zugriff auf relevante Informationen und gibt nicht, wie bei der Onlinedurchsuchung, Aufschluss über das gesamte „digitale Leben“ der letzten Jahre. Dadurch bleibt die digitale Intimsfäre der Betroffenen geschützt und die Grundordnung der freiheitlich-demokratischen Gesellschaft gewahrt. Sollte es dennoch nötig sein auf die auf einem Computer gespeicherten Daten zuzugreifen, so besteht außerdem noch die klassische Wohnungsdurchsuchung bzw. Beschlagnahme der Rechner als Option. So wird sowohl der Zugriff auf die gesuchten Daten sichergestellt, als auch den Betroffenen die Möglichkeit gegeben, einen Rechtsbeistand heranzuziehen.

Wenn man von der rechtlichen Bedenklichkeit der Onlinedurchsuchung einmal absieht, verbleiben immer noch große Probleme bei der technischen Umsetzung. Betrachtet man diese, bekommt man den Eindruck, dass es sich hierbei um von Laien entwickelte Ideen handelt, die lediglich auf deren eigenem Erfahrungshorizont beruhen. Bei fast allen Vorgehensweisen wird darauf vertraut, dass es sich bei den Verdächtigen um sehr naive Personen handelt, die Spam-E-Mails nicht erkennen, sich auf dubiose Websites locken lassen, über veraltete Software verfügen und keinerlei Sicherheitsmaßnahmen ergreifen.

In der Praxis sind für eine Onlinedurchsuchung bestimmte Voraussetzungen nötig. Dazu gehören zu allererst fundierte Kenntnisse über das zu infiltrierende Zielsystem. Diese umfassen nicht nur Informationen über das verwendete Betriebssystem (bzw. verwendete Betriebssysteme und virtuelle Maschinen), eine evtl. vorhandene Festplattenverschlüsselung und die Antwort auf die Frage, ob überhaupt beschreibbare Speichermedien eingesetzt werden[11]. Sondern ebenfalls Details über auf dem System installierte Software, sowie ggf. Firewalls, Anti-Malware-Programme, Passwörter usw.

Diese Informationen sind allerdings wertlos, wenn nicht darüber hinaus das Verhalten der Zielperson im Vorfeld analysiert wird. Es ist nicht nur wichtig zu wissen, welche Websites wann besucht werden, sondern auch, ob die zu überwachende Person E-Mail-Anhänge öffnet, Scripte auf Websites startet oder Passwörter speichert. Erst wenn dies alles bekannt ist, kann überhaupt mit der Fertigung der Remote Forensic Software begonnen werden, die wohl in der Regel eine teure „Maßanfertigung“ für das Zielsystem seien dürfte. Und selbst wenn alle diese Hürden erfolgreich überwunden würden, bliebe noch das Problem der Installation auf dem Zielrechner, wobei einzig das Eindringen in die Wohnung ein realistisches Szenario darstellt. Rechtlich ist dies aber nicht zulässig.

Zusammenfassend lässt sich feststellen, dass es Alternativen zur Onlinedurchsuchung gibt, mit denen sich für ein Ermittlungsverfahren relevante Informationen mindestens genauso gut erheben lassen. Dazu gehört z. B. die Wohnungsdurchsuchung bzw. Beschlagnahme von verdächtigen Datenträgern, für die nicht einmal eine Gesetzesänderung notwendig gewesen wäre. Und letztlich muss außerdem bedacht werden, dass sich die Onlinedurchsuchung mit einem ganz simplen Mittel verhindern lässt, von welchem mit an Sicherheit grenzender Wahrscheinlichkeit das Gros der Kriminellen Gebrauch machen wird: Das Trennen der Leitung.

4 Vorratsdatenspeicherung

4.1 Motivation

Eine Lagerung von (im weitesten Sinne) Daten auf Vorrat ist per se nichts ungewöhnliches. In Schulen und Universitäten werden beispielsweise Prüfungen für ein bis zwei Jahrzehnte aufbewahrt, das Bundeszentralregister in Bonn speichert u. a. Informationen über strafgerichtliche Verurteilungen für eine bestimmte Zeit und bei Verstößen gegen die Straßenverkehrsordnung

11 Denkbar wäre auch, dass die Zielperson zum Arbeiten immer eine Live-Umgebung von einer CD bootet. Das Betriebssystem müsste somit nach jedem Bootvorgang erneut infiltriert werden und alle im Speicher gesicherten Daten gingen nach einem Neustart des Rechners verloren.

erhält man „Punkte“ im Verkehrszentralregister in Flensburg. Alle diese klassischen „Datenspeicher“ weisen zwei typische Merkmale auf: Zum Einen sind die Daten meist in herkömmlichen Akten gespeichert und/oder der Zugriff auf diese ist erst auf Antrag möglich. Es gibt folglich keinen unmittelbaren Zugang zu den Informationen. Und zweitens sind die erwähnten Register transparent. Jede Bürgerin und jeder Bürger hat also das Recht einen Auszug der eigenen Einträge zu erhalten.

Im Gegensatz dazu geht die in diesem Kapitel behandelte Vorratsdatenspeicherung einen ganz neuen Weg. Einer der wichtigsten Unterschiede ist, dass die Informationen einzig elektronisch – also imaginär – gespeichert werden. Aufgrund der riesigen Datenflut kann niemand mehr genau sagen, auf welchem fysikalischen Datenträger welcher Eintrag liegt. Die Informationssicherung wird damit komplett dem Computersystem überlassen und ist für Außenstehende intransparent. Hinzu kommt, dass durch die Vernetzung der Datenbanken mit den Rechnern der Behörden eine Datenabfrage unmittelbar sowie praktisch ohne Kosten- und Personalaufwand möglich ist. Technisch ist es folglich ohne Weiteres machbar, das Kommunikationsverhalten der gesamten Bevölkerung auszuwerten. Und letztlich wird mit dem Prinzip der Registertransparenz gebrochen, da die von der Vorratsdatenspeicherung Betroffenen keine Möglichkeit haben die erhobenen Daten einzusehen.

Nachfolgend wird zuerst die aktuelle Gesetzeslage betrachtet und danach näher auf die Rechtsprechung eingegangen, gefolgt von Erläuterungen zur technischen Umsetzung. Ein Fazit schließt das Kapitel ab.

Zum Einstieg in das Thema eignen sich außerdem die Website des Arbeitskreises Vorratsdatenspeicherung [AKVo09], eine Folge des Chaosradios Express [CRE051] sowie das Vorlesungsscript zum Thema „Internetrecht“ von Prof. Dr. Thomas Hoeren [Hoer08].

4.2 Gesetzeslage

Mit „*Vorratsdatenspeicherung in der Telekommunikation*“ (nachfolgend kurz „Vorratsdatenspeicherung“ genannt) wird die gesetzliche Verpflichtung aller Anbieter von elektronischen Dienstleistungen bezeichnet, bestimmte Kommunikationsdaten unabhängig von einem Verdacht für den Zeitraum von ca. sechs Monaten[12] zu speichern. Diese Daten dürfen nur zur Abwehr von Gefahren, zur Verfolgung von Straftaten und für die Arbeit der Geheimdienste zur Verfügung gestellt werden. Das entsprechende Unternehmen darf die Daten somit nicht für eigene Zwecke nutzen. Die Vorratsdatenspeicherung trat mit der Novelle des *Telekommunikati-*

12 Die Speicherdauer beträgt mindestens sechs und höchstens sieben Monate.

onsgesetzes (*TKG*) am 1. Januar 2008 in Kraft [Hoer08], mit welcher eine entsprechende unionseuropäischen Richtlinie umgesetzt worden ist [§VDS06]. Die gesetzliche Verpflichtung gilt seit dem Ende der Übergangsfrist, dem 1. Januar 2009.

Bis Ende 2007 galt eine Regelung, welche die Speicherung von verbindungsrelevanten Daten weitestgehend unterband. Zwar ermöglichte die alte Fassung des TKGs den Providern die Speicherung der Anschluss- und Berechtigungskennungen, des Verbindungszeitraums etc. Allerdings mussten alle Daten sofort nach Beendigung der Kommunikation gelöscht werden, sofern sie nicht für den Aufbau weiterer Verbindungen relevant waren oder für Abrechnungszwecke benötigt wurden. Das bedeutet, dass z. B. dynamische IP-Adressen[13] bei Flatratetarifen nicht gesichert werden durften und alle Daten in der Regel nach Erhalt der Rechnung endgültig gelöscht wurden [LGDA05].

Die ICT-Dienstleistungsunternehmen sind nach dem novellierten TKG im Einzelnen verpflichtet folgende Daten zu speichern [§TKÜ07]:

- Bei **Telefongesprächen** die *Rufnummern* oder andere Kennungen der anrufenden und der angerufenen Person, sowie ggf. *Kennungen von Um- bzw. Weiterschaltungen*. Außerdem *Datum* und *Uhrzeit* von Beginn und Ende der Verbindung.
- Bei **Mobilfunkgesprächen** darüber hinaus die *internationalen Teilnehmerkennungen* der Beteiligten sowie die *internationalen Kennungen der Endgeräte*. Ferner noch die Bezeichnung der beiden zu Beginn der Verbindung genutzten *Funkzellen* und deren *geografische Position*.
- Bei **Voice-over-IP**-basierten (VoIP) Gesprächen schließlich auch die *IP-Adressen* der beiden beteiligten Anschlüsse.
- Bei der Versendung und beim Empfang von E-Mails und anderen **elektronischen Nachrichten** die *Absenderadresse*, *alle Zieladressen* sowie die *IP-Adresse* des Senders, *Datum* und *Uhrzeit*.
- Beim Zugriff auf ein **elektronisches Postfach** dessen *Kennung* sowie die *IP-Adresse*, von der die Abfrage gestartet worden ist, *Datum* und *Uhrzeit*.
- Bei der Nutzung des **Internets** die vergebene *IP-Adresse* sowie eine eindeutige *Anschlusskennung*. Außerdem *Datum* und *Uhrzeit* von Beginn und Ende der Verbindung.

Die Speicherung erfolgt nicht nur bei erfolgreichem Verbindungsaufbau, sonder ebenfalls bei unbeantworteten Anrufen oder bei – z. B. aufgrund von Netzwerkstörungen – erfolglosen Verbindungsversuchen. Die Vorratsdatenspeicherung gestattet ausdrücklich nicht die Sicherung

13 „Internet Protocol Address“. Engl.: „Internetprotokolladresse“. Logische Netzwerkadresse.

von Kommunikationsinhalten.

Die von den Dienstanbietern erhobenen Daten müssen so gespeichert werden, dass sie vor unbefugtem Zugriff geschützt sind. Auskunftsersuche der Geheimdienste oder der Polizeien müssen darüber hinaus unverzüglich beantwortet werden. Außerdem hat die Speicherung der Daten auf einem System innerhalb der Grenzen der Europäischen Union zu erfolgen.

4.3 Rechtsprechung

Über die Frage inwieweit das neue Telekommunikationsgesetz bzw. die Vorratsdatenspeicherung im Speziellen verfassungsgemäß ist, liegt aktuell (29. Januar 2009) noch keine endgültige Entscheidung vor. Geltung haben allerdings mehrere Aussetzungsbeschlüsse und Einschränkungen.

Wie das Bundesverfassungsgericht am 11. März 2007 urteilte [BVG208], ist die Speicherung von verbindungsrelevanten Daten an sich kein Eingriff in die Freiheit der BürgerInnen. Der Abruf und die Verwendung dieser Daten hingegen schon, da so die Möglichkeit besteht, weit reichende Kenntnisse über das Kommunikationsverhalten einerseits und über soziale Kontakte andererseits zu erlangen [Hei108][n-tv08]. Dies hat zur Folge, dass die Speicherung der Kommunikationsdaten zwar nicht ausgesetzt wird, die Verbindungsinformationen aber lediglich zur Verfolgung von schweren Straftaten genutzt werden dürfen. Ferner muss der Verdacht gegen die betroffenen Personen begründet und die Nutzung anderer Mittel zur Beschaffung der benötigten Kenntnisse schwer oder aussichtslos sein. Dieses Einschränkung wurde zunächst auf sechs Monate befristet und die Bundesregierung beauftragt, bis September 2008 einen Bericht über die praktischen Folgen der Vorratsdatenspeicherung vorzulegen. Da dies nicht geschehen ist, wurde in einem zweiten Urteil vom 1. September 2008 die Einschränkung um ein weiteres halbes Jahr verlängert [Hei208].

Eine weitere Beschränkung der Vorratsdatenspeicherung nahm das BVerfG mit dem Urteil vom 28. Oktober 2008 vor. Zwar wurde auch hier die Erhebung der Daten nicht angetastet, die Verwendung jedoch an sehr enge Bedingungen geknüpft [Hei308][BVG308]. So darf der Abruf der Daten seitdem nur noch zur Abwehr einer dringenden Gefahr für Leib, Leben oder die Freiheit einer Person, den Bestand des Bundes oder eines Landes erfolgen. Außerdem bei gemeinen Gefahren[14]. Die Daten dürfen auch zur Strafverfolgung genutzt werden, allerdings nur, wenn es sich um so schwere Delikte handelt, dass auch eine Telekommunikationsüberwachung erlaubt wäre. Begründet wird das Urteil u. a. damit, dass durch die derzeitige Form des

14 Eine „gemeine Gefahr“ ist eine Gefahr für eine unbestimmte Anzahl von Personen, z. B. bei Naturkatastrofen [Lexe09].

TKGs bei einer Maßnahme zur Gefahrenabwehr evtl. auch Personen erfasst würden, die mit der Ursache nichts zu tun haben. Außerdem wurde bemerkt, dass durch den weiten abrufberechtigten Behördenkreis für die Betroffenen die Wahrscheinlichkeit steigt, weiteren Überwachungsmaßnahmen ausgesetzt zu werden. Dies schränke das Vertrauen sowohl in den im Grundgesetz verankerten Schutz der Telekommunikation[15], als auch die allgemeine Unbefangenheit des elektronischen Informations- und Gedankenaustauschs ein.

Durch das Urteil sind des Weiteren die Befugnisse der Geheimdienste beschränkt worden. Die VerfassungsrichterInnen hielten den generellen Zugriff der Nachrichtendienste auf die Telekommunikationsdaten für schwer überschau- und abgrenzbar. Da die Verbindungsdaten verdachtsunabhängig gespeichert werden müssen, wäre es so relativ leicht möglich, in den Fokus des Verfassungsschutzes zu geraden. Der Zugang zu den Daten unterliegt deshalb auch hier den oben genannten strengen Auflagen.

Am 1. März 2009 endet für die Bundesregierung die Frist, um den Bericht über die praktischen Folgen der Vorratsdatenspeicherung vorzulegen. Danach ist mit einem endgültigem Urteil des Bundesverfassungsgerichts zu rechnen.

4.4 Technische Umsetzung

Da die Novelle des TKGs erst am 31. Dezember 2007 im Bundesgesetzblatt veröffentlicht wurde, das Gesetz jedoch bereits einen Tag später in Kraft getreten ist, war eine sofortige Umsetzung der Vorratsdatenspeicherung technisch nicht möglich. Im Vorfeld wurde daher eine Übergangsfrist von einem Jahr vereinbart.

Bei der allgemeinen Realisierung ließen sich die Provider unterschiedlich viel Zeit. Das zur Telefónica gehörende Mobilfunkunternehmen O2 hatte die Regelung bereits 2007, also vor Verabschiedung des Gesetzes, umgesetzt. Andere Gesellschaften, wie z. B. die Deutsche Telekom, hatten zumindest bis August 2008 die Vorratsdatenspeicherung noch nicht eingeführt [Net108].

Die technische Umsetzung der Vorratsdatenspeicherung ist teilweise mit Schwierigkeiten verbunden. Vergleichsweise einfach gestaltet sich noch die Speicherung der Verbindungsdaten für die Festnetztelefonie, da hier die bestehenden Systeme theoretisch nur erweitert werden müssten. Bei den Mobilfunkdaten muss darüber hinaus noch eine Datenbank mit Standortinformationen eingebunden werden. Zu kompletten Neuerrichtungen von IT-Systemen kommt es dagegen im Bereich der E-Mail-, VoIP- und Internetverbindungsdaten. Die Verwaltung

15 Art. 10 GG: Brief-, Post- und Fernmeldegeheimnis.

dieser wird von den Providern teils selber übernommen, teils wurde die Aufgabe der Vorratsdatenspeicherung aber auch ausgegliedert und anderen Firmen überlassen.

Offen ist zu diesem Zeitpunkt (29. Januar 2009) noch, in welchem Format die Verbindungsdaten gesichert werden müssen, da die Bundesnetzagentur bisher keine Richtlinie dazu vorgelegt hat [Net208]. Dies führt zu der absurden Situation, dass alle Dienstanbieter zwar seit mindestens Januar 2009 Daten speichern, diese Daten zu einem späteren Zeitpunkt jedoch noch konvertiert werden müssen. Sollte dies technisch nicht möglich sein, weil z. B. das gewählte Format mit dem neuen vollkommen inkompatibel ist, handelt der Provider rechtswidrig, obwohl er vorher keine Möglichkeit hatte, seine Systeme anzupassen. Darüber hinaus ist das automatisierte Auskunftsverfahren ebenfalls nicht standardisiert, da die Bundesnetzagentur hier noch keine Richtlinie zur Verfügung stellt [BNA_09].

Sicher ist hingegen, dass durch die Vorratsdatenspeicherung für die betroffenen Unternehmen Kosten in Millionenhöhe entstanden sind bzw. noch entstehen werden. Konkrete Zahlen liegen aktuell (29. Januar 2009) noch nicht vor, Schätzungen gehen aber davon aus, dass sich die Gesamtkosten für die Anschaffung der Hard- und Software allein auf über 330 Mio. Euro belaufen werden [eco_08]. Eine Aufwandsentschädigung für das Speichern der Daten ist bisher nicht vorgesehen. Sollten gerichtliche Klagen gegen diesen Zustand erfolglos bleiben, ist davon auszugehen, dass die Provider die durch die Vorratsdatenspeicherung verursachten Zusatzkosten an die Kundschaft weiterreichen werden.

4.5 Fazit

Betrachtet man die Urteile des Bundesverfassungsgerichts, so sind Analogien zur Onlinedurchsuchung deutlich erkennbar. Kurz zusammengefasst lautet die Bewertung der RichterInnen: der Gesetzgeber hat sich zu weit aus dem Fenster gelehnt. Der Wunsch der Bundesregierung, nahezu jeder Polizeibehörde und allen Geheimdiensten praktisch uneingeschränkten Zugriff auf alle Telekommunikationsdaten zu gewähren, ist damit vom Tisch. Verwenden dürfen die entsprechenden Behörden die gesammelten Daten in Zukunft nur in wenigen Ausnahmefällen. Und zwar insbesondere dann, wenn sie ohnehin von anderen Maßnahmen, wie einer Telekommunikationsüberwachung, Gebrauch machen könnten. Ob das Gesetz damit überhaupt noch sinnvoll ist, sei dahingestellt.

Gegen den anderen Aspekt der Vorratsdatenspeicherung, nämlich das Sammeln der Daten an sich, hat das Gericht bisher keine Einwände, was insbesondere Bürgerrechtsverbände weiter gegen das TKG Sturm laufen lässt. Dabei ist es gerade die verdachtsunabhängige Speicherung

von nahezu allen Kommunikationsverbindungen, die das Gesetz gefährlich macht. Es ist nicht nur der Generalverdacht, bei dem alle prinzipiell verdächtig sind bis das Gegenteil bewiesen ist. Hinzu kommt noch, dass dank der Vernetzung der Systeme ein Filtern nach relevanten Informationen, ähnlich der Rasterfahndung, in Sekundenbruchteilen möglich ist. Der Zeit- und Personalaufwand wird durch die elektronische Fernabfrage für die Behörden minimiert, wodurch auch die Kosten gegen Null gehen und ein flächendeckender Einsatz zumindest technisch und wirtschaftlich denkbar wäre. Jede Diktatur würde sich über ein solches Mittel freuen.

Ein weiterer kritischer Aspekt an der Vorratsdatenspeicherung ist die Gewährleistung des Datenschutzes. Das Telekommunikationsgesetz schreibt vor, dass sie Speicherung der Informationen so zu erfolgen hat, dass ein Zugriff dritter ausgeschlossen ist. Da insbesondere kleine Provider, um die immensen Mehrkosten zumindest teilweise zu reduzieren, die Aufgabe der Datenspeicherung outsourcen werden, können weder sie selber noch eine Behörde die tatsächliche Sicherheit überprüfen. Doch auch die Anbieter, die ihre Verkehrsdaten selber speichern, sind vor Fehlern und Sicherheitslücken nicht gefeit. Allein die hohe Zahl an Unternehmen und die Menge an Informationen lässt vermuten, dass es wahrscheinlich öfters zu „Datenpannen“ kommen wird.

Unabhängig davon, ob nur Behörden auf die bevorrateten Daten zugreifen, oder ob diese absichtlich oder versehentlich anderweitig verwendet werden, die Vorratsdatenspeicherung ist ein weiterer Schritt auf dem Weg zum „Gläsernen Menschen“. Sie erlaubt die nahezu lückenlose Analyse des sozialen Netzes, gibt Hinweise zum Beruf, zur Freizeitgestaltung und ggf. zur gesundheitlichen Verfassung. Außerdem besteht die Möglichkeit Bewegungsprofile zu erstellen. All diese Informationen sind nicht nur für die Nachrichtendienste interessant, sondern ließen sich auch für viel Geld verkaufen.

Und letztlich bleibt festzustellen, dass die Vorratsdatenspeicherung für die Gefahrenabwehr und die Strafverfolgung de facto wertlos ist. Zwar können auch Schwerstkriminelle die eigentliche Speicherung der Daten nicht verhindern, es lässt sich jedoch mit einfachen Mitteln eine Zuordnung zur eigenen Person vermeiden. Reguläre Telefongespräche können immer noch von einer Telefonzelle aus abgesetzt werden und für die mobile Kommunikation eignen sich gestohlene Handys oder Prepaidkarten, die nicht auf den eigenen Namen registriert und nur kurzzeitig in Benutzung sind. Wer über das Web kommuniziert, geht in eines der unzähligen Internetcafés und E-Mail-Konten werden ganz einfach häufig gewechselt. Wem dies alles zu viel Aufwand ist, dem bleibt des Weiteren die Möglichkeit, extrem viele Datensätze zu produzieren. Zwei Terroristen, die jeden Tag mehrfach miteinander telefonieren, generieren einen nahezu

wertlosen Eintrag, sofern nur einzelne Gespräche für die Ermittlungen relevant sind. Ähnliches gilt für das Abrufen und das Versenden von E-Mails, sowie für Verbindungen ins Internet. Werden die elektronischen Postfächer alle fünf Minuten automatisch überprüft, ist nicht mehr nachzuweisen, wann eine bestimmte Nachricht abgerufen wurde. Wird mit einer bestimmten Person viel kommuniziert, so geht eine einzelne verdächtige E-Mail schlicht unter. Und bei Flatratetarifen für die Internetverbindung kommt es bei den meisten Providern lediglich zu einem täglichen Verbindungsabbruch und -wiederaufbau, was die Erfassung der Verbindungsdauer in diesem Fall sinnlos macht.

5 Rechtliches zu WLANs

5.1 Motivation

Seit Anfang des 21. Jahrhunderts gewinnt die mobile Kommunikation im Bereich der Computernetze mehr und mehr an Bedeutung. So sind bereits 2005 in der Europäischen Union mehr Laptops als Desktoprechner verkauft worden, und der Großteil davon verfügte bereits über eingebaute Funknetzwerkkarten [Bund07]. Gleichzeitig stieg die Anzahl der breitbandigen Internetanschlüsse rasant an. Dies führt dazu, dass sich gerade im Heimbereich WLANs zusehends durchsetzen und die als unpraktisch geltende kupferbasierte Verkabelung weitestgehend ablösen.

Doch so vorteilhaft eine Funkverbindung auch ist, sie birgt grundsätzlich einige gravierende Nachteile. Der wohl wichtigste ist hier die Reichweite des Signals. Denn während beim herkömmlichen Ethernet lediglich Rechner mit dem LAN verbunden werden können, wenn sie mit einem Kabel an dieses angeschlossen sind, so deckt die Luftschnittstelle ein bestimmtes Gebiet ab. Alle Geräte in diesem Gebiet sind theoretisch in der Lage im WLAN zu kommunizieren, was üblicherweise auch Nachbarwohnungen und ggf. einen Teil des öffentlichen Raumes – z. B. Straßen und Gehwege – mit einschließt.

Diese Tatsache eröffnet gerade Kriminellen ganz neue Möglichkeiten. Die zwei bekanntesten Missbrauchspotenziale, das „Schwarzsurfen“ über einen fremden Internetanschluss und die Störerhaftung bei Rechtsverletzungen durch andere, werden in diesem Kapitel näher behandelt. Da beide Themen sich inhaltlich ähneln und teilweise überschneiden, wurden sie in einem Kapitel zusammengefasst. Bei jedem wird zunächst die Gesetzeslage erläutert, dann auf die Rechtsprechung eingegangen und schließlich die technische Seite beleuchtet. Am Schluss fasst ein Fazit beide Bereiche zusammen und bewertet diese.

Um tiefer in beide Themen einzusteigen sei an dieser Stelle die Website „Schwarz-Surfen.de“ empfohlen [Fern09].

5.2 Gesetzeslage zum „Schwarzsurfen“

Umgangssprachlich wird das unbefugte Einloggen in ein fremdes Funknetzwerk und die Nutzung eines damit verbundenen Internetzugangs als „Schwarzsurfen“ bezeichnet. Es existiert in der Bundesrepublik noch keine eindeutige Gesetzeslage bzw. Rechtsprechung zum Thema, jedoch wird das unbefugte Eindringen in ein fremdes WLAN allgemein als strafbar eingeschätzt. Dabei ist es erst einmal unerheblich, ob das WLAN durch eine Verschlüsselung o. ä. gesichert ist oder nicht.

Das Amtsgericht Wuppertal hat, wie im nachfolgenden Abschnitt näher erläutert wird, das unbefugte Einloggen in ein ungeschütztes WLAN für illegal erklärt. Es verstößt gegen das Abhörverbot, den Datenschutz und stellt außerdem, sollte kein Entgelt entrichtet werden, eine Bereicherung dar [ITRM08]. Da dies im beschriebenen Fall mit Absicht geschah, kam es zu einer Verurteilung. Eher geringe Aussichten auf Erfolg werden wahrscheinlich aber Klagen haben, bei denen das Eindringen in ein fremdes und ungesichertes WLAN unbeabsichtigt und/oder automatisch erfolgt ist, sofern kein Schaden angerichtet wurde [ITtB06].

Anders ist die rechtliche Situation, wenn eine Sicherheitshürde eingebaut worden ist. Wird das WLAN z. B. durch eine Verschlüsselung geschützt, ist eine Überwindung dieser Zugangssicherung strafbar[16] [§StG08]. Dringt jemand nicht nur in ein Funknetzwerk ein, sondern greift auch auf gespeicherte Daten zu, wird ferner eine strafbare Veränderung der Daten riskiert[17].

5.3 Rechtsprechung zum „Schwarzsurfen“

Zum Thema „Schwarzsurfen“ liegt derzeit (29. Januar 2009) lediglich ein rechtskräftiges Urteil des Amtsgerichts Wuppertal vor [AGWu07]. In dem behandelten Fall wurde ein junger Mann angeklagt, der ein Funknetzwerk in der Nachbarschaft seiner Eltern nutzte, um ohne vorherige Absprache und ohne Zahlung eines Entgeltes eine Verbindung zum Internet aufzubauen. Der Besitzer des Internetanschlusses bemerkte die unbefugte Nutzung des Netzes und erstattete Anzeige.

Nach Auffassung des Gerichts hat der Angeklagte mit seiner Tat gegen mehrere Paragrafen

16 § 202a StGB: Ausspähen von Daten.
17 § 303a StGB: Datenveränderung.

des Telekommunikationsgesetzes verstoßen [§TKG07]. Zuerst wird hier das *Abhörverbot*[18] genannt, nach welchem es nicht zulässig ist mit einer Funkanlage Nachrichten abzuhören, die nicht für einen selbst oder die Allgemeinheit bestimmt sind. Demnach war nicht einmal der Bezug einer IP-Adresse legal, da dies informationstechnisch einer Nachricht entspricht und der Angeklagte außerdem nicht zum legitimierten Nutzungskreis gehörte.

Darüber hinaus lag eine *Bereicherung*[19] zusammen mit einem Verstoß gegen den *Datenschutz*[20] vor [§BDS06]. Der Angeklagte hatte demnach unbefugt personenbezogene Daten abgerufen, die nicht allgemein zugänglich waren. Nach Einschätzung des Gerichts fällt bereits die vom Anbieter zugewiesene IP-Adresse des Routers und die Zugangsdaten in diese Kategorie. Ferner hatte der junge Mann nicht vor, für die Nutzung des Zugangs zu bezahlen und nahm billigend in Kauf, dass durch sein Verhalten beim Kläger Kosten anfallen könnten.

Da die bisherige Rechtslage ungeklärt war, wurde lediglich eine Verwarnung ausgesprochen. Sollte der Angeklagte die Tat wiederholen, ist er zu einer Zahlung von 20 Tagessätzen à fünf Euro verpflichtet. Der verwendete Computer und das Netzgerät wurde als Tatwerkzeug eingezogen.

5.4 Technische Aspekte zum „Schwarzsurfen“

Um rechtlich auf der sicheren Seite zu sein und um das eigene Netzwerk zu schützen, ist es grundsätzlich zu empfehlen, bei der Verwendung eines Funknetzes Sicherheitsmaßnahmen zu ergreifen. Hierfür bieten handelsübliche WLAN-Access-Points normalerweise vier Optionen:

Am wichtigsten ist die Verwendung einer Verschlüsselung. Falls der Datenverkehr mitgeschnitten werden sollte, sind die Daten so immer noch wertlos, bis der eingesetzte Schlüssel ermittelt ist. Diese Ermittlung kann nur von ExpertInnen durchgeführt werden und nimmt in der Regel einige Zeit in Anspruch. Personen, die den Schlüssel nicht kennen, haben auch keine Möglichkeit sich mit dem Funknetzwerk zu verbinden. Ein regelmäßiger Wechsel des Schlüssels erhöht zusätzlich die Sicherheit.

Eine weite Maßnahme zur Verbesserung der Sicherheit ist die Unterdrückung des *Netzwerknamens* (*Service Set Identifier*, *SSID*). Wird dieser nicht ausgesendet, finden regulären Clients das WLAN nicht automatisch. Durch manuelle Eingabe der SSID ist das Einloggen ins Netz aber jederzeit problemlos möglich. Der potenzielle Kreis der NutzerInnen lässt sich schon damit erheblich reduzieren und eine automatische Anmeldung von fremden Systemen

18 §§ 89 TKG.
19 §§ 44 BDSG.
20 §§ 43 (2) BDSG.

ausschließen.

Zusätzlich beinhalten die meisten Router einen DHCP-Server, bei dem der zu vergebende IP-Adressraum begrenzt werden kann. Werden nur so viele Adressen zugelassen wie Geräte im Haushalt vorhanden sind, sinkt die Wahrscheinlichkeit, dass sich eine weitere Person Zugang zum Netzwerk verschaffen kann. IP-Adressen können zwar auch manuell eingestellt werden, hierfür ist aber vorab eine Analyse der übermittelten Daten von Nöten.

Letztlich bieten die meisten Geräte auch die Option einer MAC-Adressen-Filterung[21]. So ist es möglich, lediglich registrierten Geräten den Zugang zum Netzwerk zu gewähren. Zwar lassen sich MAC-Adressen ohne Weiteres fälschen, allerdings ist auch dies nicht ohne Fachkenntnisse möglich.

Dringt jemand in ein wie beschrieben gesichertes WLAN ein, ist dies eindeutig eine Straftat. Wurde hingegen auf Schutzmaßnahmen verzichtet, kann das versehentliche manuelle oder automatische Einloggen wahrscheinlich nicht geahndet werden. Gerade die Verwendung eines DHCP-Servers[22] in Kombination mit der Aussendung der SSID kommt technisch einer Einladung gleich, dem Netzwerk beizutreten.

5.5 Gesetzeslage zur Störerhaftung

In der Bundesrepublik Deutschland wird die Verantwortlichkeit eines Handlungs-, Zustands- oder Mitstörers als *Störerhaftung* bezeichnet. Das Sachenrecht im *Bürgerlichen Gesetzbuch* (*BGB*) besagt, dass jemand, der eine Tat nicht begangen und nicht an ihr teilgenommen hat, unter Umständen trotzdem für diese haftbar gemacht werden kann [§BGB08]. Dies ist der Fall, wenn die Person durch ihr Handeln entweder willentlich oder unabsichtlich zur Herbeiführung einer Schutzverletzung beigetragen hat[23].

Für den Betrieb von Funknetzwerken gibt es keine gesonderte Gesetzeslage, sondern es wird in der Rechtsprechung auf die existierende zurückgegriffen. Da insbesondere WLANs theoretisch von unbekannten genutzt werden können um Schutzrechtsverletzungen zu begehen, wird die klassische Störerhaftung auch hier angewendet. Meistens sind heutzutage illegal hoch- und heruntergeladene Audio- und Videodateien der Auslöser für eine Anklage.

Wird eine solche Schutzrechtsverletzung festgestellt, gerät in der Praxis zunächst die

21 „Media Access Control Address“. Engl.: „Medienzugriffskontrolladresse“. Eindeutige Hardwareadresse des Netzwerkcontrollers.

22 „Dynamic Host Configuration Protocol Server“. Engl. in etwa: „Server für das dynamische Leitrechnerkonfigurationsprotokoll“. System, das mit ihm verbundenen Rechnern automatisch IP-Adressen zuweist. Ist meistens in handelsübliche WLAN-Router integriert.

23 Adäquat kausales Verhalten [LUWK09].

Person ins Visier der Ermittlungen, auf deren Namen der Internetanschluss angemeldet ist. Kann sie nachweisen oder glaubhaft machen, dass sie die Tat nicht begangen hat, muss überprüft werden, ob eine Störerhaftung in Frage kommt. Der gängigen Rechtsprechung nach zu urteilen, ist dies vor allem dann der Fall, wenn ein ungeschütztes WLAN betrieben wird und zudem das Funknetzwerk noch seine SSID aussendet. Ein Betreiber eines geschützten Funknetzes ist bisher hingegen noch nicht verurteilt worden.

Rechtlich umstritten ist die Frage, inwieweit beim Missbrauch von fremden WLANs das *Telemediengesetz* (*TMG*) zur Geltung kommt, da es in keinem bisher gefällten Urteil berücksichtigt worden ist [LeLe08][§TMG07]. Das TMG besagt, dass ein Dienstanbieter (also in diesem Fall die Person, die ein WLAN betreibt) für die über ihr Netz übertragenen Informationen nicht verantwortlich ist, sofern er die Übermittlung nicht selbst veranlasst, den Adressaten nicht selbst ausgewählt hat und die Informationen nicht verändert worden sind[24].

Eine einheitliche Rechtsprechung und eine eindeutige Gesetzeslage besteht folglich zur Zeit nicht. Es ist zu erwarten, dass entweder hohe gerichtliche Instanzen den Sachverhalt deutlich machen, oder ein Gesetz Klarheit schafft.

5.6 Rechtsprechung zur Störerhaftung

Zur Störerhaftung liegen eine Vielzahl von Urteilen vor, die allerdings nur bedingt unterschiedlich ausfallen [Fern09]. So musste beispielsweise eine Frau für eine Urheberrechtsverletzung haften, von deren Anschluss aus Musikdateien über einen Filesharingdienst verschickt worden sind [LGHH06]. Die Frau selber bestritt die Tat, sie hatte allerdings zu diesem Zeitpunkt ein ungeschütztes WLAN betrieben. Zwar konnte nicht nachgewiesen werden wer der eigentliche Täter war. Das Gericht verurteilte die Frau dennoch, da sie an der rechtswidrigen Beeinträchtigung mitgewirkt hatte. Ihr hätte bekannt sein müssen, dass Urheberrechtsverletzungen über Filesharingdienste in den vergangenen Jahren zugenommen haben und dass ein ungeschütztes Funknetzwerk von unbekannten Dritten genutzt werden kann. Das Argument, dass die Angeklagte über fehlendes technisches Verständnis verfügte und von den Möglichkeiten der illegalen Musikverbreitung nichts wusste, entlasteten sie nicht. Sie hätte sich informieren müssen.

Ähnlich argumentierte das Gericht in einem Rechtsstreit zwischen einem Mann und einem Musiker, der seine Urheberrechte verletzt sah [LGDü08]. Über den Internetanschluss des Mannes wurden Musikstücke illegal verbreitet. Dieser versicherte eidesstattlich, dass er die hierfür erforderliche Software nicht besaß. Über das ungeschütztes WLAN des Mannes

24 § 8 TMG.

konnten aber unbekannte Dritte eine Verbindung mit dem Internet herstellen. Analog zum obigen Fall meinte das Gericht, der Mann hätte als Betreiber eines WLANs zumutbare Maßnahmen ergreifen müssen, um Rechtsverletzungen über seinen Internetanschluss zu unterbinden. Dies folgt aus dem Umstand, dass der Anschluss eine Gefahrenquelle darstellt, die nur der Betreiber überwachen kann.

Vergleichbares passierte auch einem Mann, über dessen Internetanschluss ebenfalls urheberrechtlich geschützte Musikdateien versendet wurden [OLGF08]. Der Unterschied zu den ersten beiden Fällen besteht allerdings darin, dass der Mann sein WLAN mit einem Schlüssel geschützt hatte und sich zum Zeitpunkt der Tat nachweislich im Urlaub befand. Eine dritte Person muss die Tat folglich begangen haben. Das Gericht befand, dass durch eine Verurteilung die Grenzen der Störerhaftung bis ins Unzumutbare erweitert worden wären.

Zusammenfassend lässt sich sagen, dass alle bisher zur WLAN-Störerhaftung gefällten Urteile in die gleiche Richtung gehen: Ergreifen die Angeklagten keine Sicherheitsmaßnahmen zum Schutz des eigenen Netzwerks vor Fremdzugriffen, so haften Sie in der Regel für den entstandenen Schaden[25]. Denn ein Internetanschluss gilt grundsätzlich als potenzielle Gefahrenquelle, über die Rechtsverletzungen getätigt werden können. Ist das WLAN hingegen ausreichend gesichert und/oder können die Betroffenen nachweisen, dass sie die Tat selber nicht begangen haben, so ist eine Verurteilung unzumutbar.

5.7 Technische Aspekte zur Störerhaftung

Um eine Haftbarmachung zu vermeiden, sollte ein WLAN nur dann betrieben werden, wenn es ausreichend gegen unbefugte Zugriffe geschützt ist. Die vier bereits beschriebenen Maßnahmen[26], also die Verschlüsselung der Übertragung, die Unterdrückung der SSID, die Minimierung des Adressraums und die Einrichtung eines Filters für MAC-Adressen, haben auch für die Vermeidung der Haftung Gültigkeit.

Darüber hinaus bieten viele Router aber noch zusätzliche Optionen, die die Wahrscheinlichkeit einer Haftung reduzieren. Eine Möglichkeit, den Zugriff auf Filesharingdienste zu verhindern, ist die Sperrung der verwendeten Ports[27]. Zwar ist dies nicht automatisch ein Hindernis, da viele Programme für den Datenaustausch auch auf andere Ports umschalten können, jedoch wird so zumindest bei Standardeinstellungen ein Sitzungsaufbau verhindert.

25 § 1004 BGB.
26 Siehe: *5.4 Technische Aspekte zum „Schwarzsurfen“*.
27 Ports sind Adresskomponenten in Netzwerkprotokollen, die eingesetzt werden, um ein Datenpaket einem Dienst zuzuordnen.

Außerdem könnte diese Maßnahme vor Gericht entlasten.

Des Weiteren bieten viele Router umfangreiche Protokollfunktionen. Ist es möglich mittels der Protokolle nachzuweisen, wann sich welcher Computer mit dem Funknetz verbunden hat, besteht auch eine gewisse Chance den Täter ausfindig zu machen. Hierfür muss lediglich die unbekannte MAC-Adresse mit denen anderer Geräte verglichen werden. Wie z. B. der des Notebooks des Nachbarn.

5.8 Fazit

Eine abschließende Beurteilung der Gesetzeslage im Bereich der Funknetzwerke ist schwierig. So ist es erst einmal zu begrüßen, dass der Betrieb eines WLANs eine gewisse Verantwortung mit sich bringt und dass die Gerichte es grundsätzlich für erforderlich halten, Sicherheitsmaßnahmen zu ergreifen. Fraglich ist hier allerdings, inwieweit „Otto Normalverbraucher“ in der Lage ist, diese Erfordernisse umzusetzen. Wird ein WLAN-Router ohne voreingestellte Verschlüsselung ausgeliefert, ist es durchaus wahrscheinlich, dass das Netzwerk in einem Modus betrieben wird, der aller Welt den Zugang zu diesem ermöglicht. Der Sinn und Zweck von Sicherheitsmaßnahmen übersteigt den technischen Horizont vieler Leute und/oder sie halten es nicht für nötig, sich nach dem ersten erfolgreichen Verbindungsaufbau weiter mit ihrem Router zu beschäftigen. Es funktioniert schließlich.

Aber auch die Rechtsprechung ist nicht ganz unproblematisch. So sind die Urteile teilweise kritisch zu sehen und vom technischen Standpunkt aus nicht ganz korrekt. So wurde der junge Mann, der sich unbefugt in das WLAN des Nachbarn eingeloggt hatte, u. a. darum verurteilt, weil er gegen den Datenschutz verstoßen hatte. Das Gericht entschied, dass die vom Anbieter des Internetzugangs zugewiesene IP-Adresse ein persönliches Datum ist, was durchaus stimmt. Nicht bedacht wurde jedoch, dass der junge Mann wahrscheinlich überhaupt keinen Zugriff auf diese IP-Adresse des Anschlusses hatte, da der Router diese lediglich für die Kommunikation nach außen nutzt. Im internen LAN regelt ein DHCP-Server die Adressvergabe.

Kritisch ist auch, dass der automatische Bezug einer IP-Adresse gegen das Abhörverbot verstößt. Zwar ist die Zuweisung einer Adresse kommunikationstechnisch eine Nachricht (bzw. mehrere), jedoch war das WLAN im besagten Fall so konfiguriert, dass es durch das Aussenden der SSID mit einem Rundfunksender gleichzusetzen ist. Zwar geschieht die Vergabe der IP-Adresse grundsätzlich individuell, allerdings war das Gesamtsystem so automatisiert, dass jeder Computer praktisch zum Beitritt des Funknetzes eingeladen worden ist.

Ähnlich sieht es bei der Störerhaftung aus. Selbstverständlich sind Verletzungen von

Schutzrechten, gerade bei Musik- und Filmdateien, zu verfolgen und zu ahnden. Ob die gängigen Urteile allerdings verhältnismäßig sind, ist fraglich. Wird beispielsweise ein Rentner zur Zahlung von mehreren tausend Euro Schadenersatz verurteilt, obwohl er nachweislich nicht der eigentliche Täter ist und von WLAN-Verschlüsselung noch nie etwas gehört hat, kann dies durchaus als übertrieben angesehen werden. Solche Urteile sind ferner kontraproduktiv, da sie zwar den unzähligen auf Abmahnungen spezialisierten Anwaltskanzleien die Taschen füllen, aber Gleichzeitig das Vertrauen der Bürgerinnen und Bürger in die Technik schwinden lassen.

Um diese Probleme zu beseitigen und eine einheitliche und eindeutige Rechtslage zu schaffen, ist eine gesetzliche Regelung die beste Lösung. Die Störerhaftung müsste hier generell ausgeschlossen werden, sofern eine Schutzrechtsverletzung nicht willentlich geschieht. Gleichzeitig sollten die Hersteller von WLAN-Access-Points verpflichtet werden, ihre Geräte ab Werk mit einer aktivierten Verschlüsselung auszuliefern, sofern dies nicht durch eine Selbstregulierung des Marktes geschieht. Erfreulicherweise scheinen viele Hersteller verstanden zu haben, dass eine voreingestellte Verschlüsselung einen Wettbewerbsvorteil darstellt und bieten ausschließlich solche Geräte an. So lässt sich der Missbrauch unzähliger privater Internetanschlüsse weitestgehend verhindern, da allein hierdurch das Eindringen unbefugter nahezu ausgeschlossen werden kann.

Wer ein offenes und ggf. sogar kommerzielles WLAN betreibt, muss von der Störerhaftung ebenfalls ausgenommen sein, sofern eine Beteiligung an einem Rechtsverstoß nicht nachweisbar ist. Hier muss das Telemediengesetz greifen, welches besagt, dass ein Dienstanbieter nicht für die übermittelten Daten verantwortlich gemacht werden kann. Jede anders lautende Regelung würde das wirtschaftliche Aus für jeden Hot-Spot-Betreiber bedeuten. Und auch Privatleute könnten durch teure Gerichtsprozesse und Schadenersatzforderungen in den Ruin getrieben werden.

6 Zusammenfassung

Im Informationszeitalter, auf das sich unsere Gesellschaft mit großen Schritten zubewegt, spielt die Informations- und Kommunikationstechnik eine entscheidende Rolle und stellt einen wichtigen Aspekt im Leben der Menschen dar. Darum ist auch das ICT-Recht von hoher Bedeutung. Umso erfreulicher ist es festzustellen, dass sich die Politik Gedanken macht, wie in Zukunft auch im „digitalen Leben“ der Rechtsstaat greift und die freiheitlich-demokratisch Grundordnung gewahrt bleibt.

Problematisch ist in diesem Zusammenhang, dass sowohl die Gesetzeslage als auch die Rechtsprechung nur teilweise auf hinreichendem technischem Verständnis fußt. Man gewinnt bei einer näheren Betrachtung leicht den Eindruck, die verantwortlichen PolitikerInnen hätten sich beim Entwurf der Gesetze entweder nur unzureichend beraten lassen, oder einfach ihren eigenen Erfahrungshorizont zu Grunde gelegt. Außerdem scheint es so etwas wie eine Folgenabschätzung bei technischen Themen grundsätzlich nicht zu geben.

Ein Beispiel hierfür ist die Onlinedurchsuchung. Vom Innenministerium angeordnet, wurde sie zunächst klein geredet, obwohl sie einen weit reichenden Einblick in die digital gespeicherten persönlichen Dokumente ermöglicht. Der Bundesgerichtshof sprach schließlich ein Machtwort und das Bundesverfassungsgericht schuf darüber hinaus noch ein neues Grundrecht auf digitale Intimsfäre. Zwar bietet die neue Gesetzeslage den Polizeien und Geheimdiensten mittlerweile wieder die Möglichkeit Onlinedurchsuchungen durchzuführen, jedoch nur in einem engen rechtlichen Rahmen. Technisch wird sich der Erfolg der Maßnahme ferner nicht einstellen, weil eine Person, die ein mittelmäßiges technisches Verständnis und einen gewissen Grad an Erfahrung besitzt, sehr wahrscheinlich nicht auf einen „Bundestrojaner“ hereinfällt.

Jedoch sind auch die Entscheidungen der Gerichte nicht immer unkritisch zu sehen. Im Falle der Vorratsdatenspeicherung erkannten sie zwar korrekt, dass ein nahezu uneingeschränkter automatisierter Zugriff auf gespeicherte Verkehrsdaten nur in wenigen Ausnahmefällen möglich sein darf. Allerdings wurde die eigentliche Datenspeicherung nicht in Frage gestellt. Dabei ist es gerade dieser Teil des Gesetzes, der die größten Schwierigkeiten bereiten wird. Mal abgesehen davon, dass sich die erfassten Daten technisch bestens dafür eignen würden, die gesamte Bevölkerung flächendeckend zu überwachen. Auch die Sicherheit der Daten wird als gegeben hingenommen. Es hätte bemerkt werden müssen, dass ein einhundertprozentiger Schutz der Kommunikationsdaten nicht realisierbar ist und es, nicht zuletzt aufgrund der hohen Anzahl an Anbietern und an gespeicherten Informationen, zwangsläufig zu „Datenpannen“ kommen wird.

Kritisch betrachtet werden muss auch die Rechtsprechung im Fall des Missbrauchs von Funknetzwerken. Die Gerichte haben hier für ihre Argumentation fast ausschließlich die Störerhaftung zu Grunde gelegt, und sind dabei häufig über das Ziel hinaus geschossen. Zwar ist es richtig und wichtig klar zu stellen, dass der Betreiber eines WLANs auch für die Sicherheit des Netzes zu sorgen hat. Allerdings sind die Urteile gegen einzelne Privatpersonen unverhältnismäßig, gerade weil sie an der eigentlichen Tat nicht beteiligt waren. Das technische Verständnis ist hier, man denke an das Beispiel des Zugriffs auf die vom Internetprovider zuge-

wiesene IP-Adresse, nicht in ausreichendem Maße vorhanden. Andererseits haben die Gerichte auch nicht viel mehr Möglichkeiten als auf die ihnen bekannte Rechtslage zurückzugreifen, da der Gesetzgeber noch kein separates „WLAN-Recht“ eingeführt hat.

Zusammenfassend lässt sich sagen, dass es zwar positiv zu werten ist, dass das Informationszeitalter allmählich auch bei den Abgeordneten angekommen ist. Die Ergebnisse der ersten gesetzlichen Maßnahmen fallen aber leider sehr spärlich aus und bedürfen noch einiger Überarbeitungen. Bleibt zu hoffen, dass die kommenden Generationen von PolitikerInnen sich mit solchen Gesetzen nicht mehr so schwer tun und Regelungen schaffen, die unsere Gesellschaft weiter nach vorn bringen, statt die Technik nur einzusetzen, um uns in längst überwundene Zeiten zurückzubringen.

Literaturverzeichnis

[AGWu07] Amtsgericht Wuppertal: "Urteil vom 3. April 2007, Az. 22 Ds 70 Js 6906/06", Schwarz-Surfen.de, 03. April 2007, http://www.schwarz-surfen.de/urteile/ag-wuppertal-03042007-22-ds-70-js-690606/.

[AKVo09] Arbeitskreis Vorratsdatenspeicherung: "Stoppt die Vorratsdatenspeicherung!", vorratsdatenspeicherung.de, 18. Januar 2009, http://www.vorratsdatenspeicherung.de/index.php.

[BNA_09] Bundesnetzagentur: "Informationen für Telekommunikationsdiensteanbieter zum Thema "Vorratsdatenspeicherung"", Bundesnetzagentur.de, 18. Januar 2009, http://www.bundesnetzagentur.de/enid/Technische_Umsetzung_von_Ma_nahmen_zur_Ueberwachung_und_zur_Auskunftserteilung_nach___ssss__TKG/Info_4hc.html.

[Bund07] Bundesregierung: "Drucksache 16/6117", Deutscher Bundestag, 23. Juli 2007, http://www.icems.eu/docs/deutscher_bundestag.pdf.

[BVG108] Bundesverfassungsgericht: "Leitsätze zum Urteil des Ersten Senats vom 27. Februar 2008", Karlsruhe, 27. Februar 2008, http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html.

[BVG208] Bundesverfassungsgericht: "Eilantrag in Sachen „Vorratsdatenspeicherung“ teilweise erfolgreich", Karlsruhe, 11. März 2008, http://www.vorratsdatenspeicherung.de/images/pm_37-08.pdf.

[BVG308] Bundesverfassungsgericht: "BvR 256/08 vom 28.10.2008", Karlsruhe, 28. Oktober 2008, http://www.bundesverfassungsgericht.de/entscheidungen/rs20081028_1bvr025608.html.

[CR_122] Chaosradio: "Folge 122: Der Bundestrojaner", Potsdam, 28. März 2007, http://chaosradio.ccc.de/cr122.html.

[CR_127] Chaosradio: "Folge 127: Der Bundestrojaner Reloaded", Potsdam, 29. August 2007, http://chaosradio.ccc.de/cr127.html.

[CR_132] Chaosradio: "Folge 132: Computerverwanzung", Potsdam, 27. Februar 2008, http://chaosradio.ccc.de/cr132.html.

[CRE051] Chaosradio Express: "Folge 51: Vorratsdatenspeicherung, Anonymität und digitale Freiräume", Berlin, 05. November 2007, http://chaosradio.ccc.de/cre051.html.

[eco_08] Verband der deutschen Internetwirtschaft eco e. V.: "Gericht: Vorratsdatenspeicherung ohne Kostenerstattung ist nicht zumutbar", Berlin, 22. Oktober 2008, http://www.eco.de/politik/202_5582.htm.

[Fern09] Ferner, D.: "Störerhaftung", Schwarz-Surfen.de, 24. Januar 2009, http://www.schwarz-surfen.de/storerhaftung/.

[Hei108] Krempl, S.: "Bundesverfassungsgericht schränkt Vorratsdatenspeicherung ein", Heise Online, 19. März 2008, http://www.heise.de/newsticker/Bundesverfassungsgericht-schraenkt-Vorratsdatenspeicherung-ein--/meldung/105284.

[Hei208] Krempl, S.: "Bundesverfassungsgericht verlängert Schranken bei Vorratsdatenspeicherung", Heise Online, 04. Septemer 2009, http://www.heise.de/newsticker/Bundesverfassungsgericht-verlaengert-Schranken-bei-Vorratsdatenspeicherung--/meldung/115469.

[Hei308] Krempl, S.: "Karlsruhe begrenzt erneut den Zugriff auf TK-Vorratsdaten", Heise Online, 06. November 2008, http://www.heise.de/newsticker/Karlsruhe-begrenzt-erneut-den-Zugriff-auf-TK-Vorratsdaten--/meldung/118495.

[Heis07] Rötzer, F.: "Innenministerium: Verfassungsschutz, MAD und BND können Online-Durchsuchungen durchführen", Heise Online, 24. März 2007, http://www.heise.de/newsticker/Innenministerium-Verfassungsschutz-MAD-und-BND-koennen-Online-Durchsuchungen-durchfuehren--/meldung/87316.

[Hoer08] Hoeren, T.: "Internetrecht", Universität Münster, Münster, September 2008, http://www.uni-muenster.de/Jura.itm/hoeren/materialien/Skript/Skript_September2008.pdf.

[ITRM08] Keller, M.: "Achtung: Schwarzsurfen ist strafbar!", IT-Recht Kanzlei Keller-Stoltenhoff, Keller, Münch, Petzold München, 23. Mai 2008, http://www.it-recht-kanzlei.de/schwarzsurfen-ist-strafbar.html.

[ITtB06] Hülskötter, M.: "Grauzone Schwarzsurfen: was erlaubt ist und was nicht", IT-tech BLOG, 22. März 2006, http://www.it-techblog.de/grauzone-schwarzsurfen-was-erlaubt-ist-und-was-nicht/03/2006/.

[LeLe08] Leis, H. / Lentföhr, C.: "Haftungsausschluss eines WLAN-Betreibers nach dem Telemediengesetz (TMG).", AdvoGarant.de, 12. Juni 2008, http://www.advogarant.de/Infocenter/Rechtsinfo/Verbraucherrecht/Allgemein/WLAN.html.

[Lexe09] Lexexakt.de: "Gefahr, dringende/erhebliche/gemeine Gefahr im Polizeirecht", Lexexakt.de, 22. Januar 2009, http://www.lexexakt.de/glossar/gefahr.php.

[LGDA05] Landgericht Darmstadt: "Urteil vom 07.12.2005; 25 S 118/2005; Speicherung von IP-Adressen", JurPC.de, 07. Dezember 2005, http://www.jurpc.de/rechtspr/20060052.htm.

[LGDü08] Landgericht Düsseldorf: "Az 12 O 195/08", Medien Internet und Recht, Düsseldorf, 16. Juli 2008, http://medien-internet-und-recht.de/pdf/VT_MIR_2008_227.pdf.

[LGHH06] Landgericht Hamburg: "Az 308 O 407/06", Medien Internet und Recht, Hamburg, 26. Juli 2006, http://medien-internet-und-recht.de/pdf/vt_MIR_Dok._191-2006.pdf.

[LUWK09] Lernen, Universität, Weiterbildung, Karriere: "Adäquat kausal", allesgelingt.de, 25. Januar 2009, http://www.allesgelingt.de/studium/rechtswissenschaft/definitionen/adaequatkausal.php.

[n-tv08] n-tv: "Vorratsdatenspeicherung - Gesetz teilweise ausgesetzt", n-tv.de, 19. März 2008, http://www.n-tv.de/936009.html.

[Net108] Meister, A.: "Vorratsdatenspeicherung: Umsetzung und Kosten", Netzpolitik.org, 19. August 2008, http://netzpolitik.org/2008/vorratsdatenspeicherung-umsetzung-und-kosten/.

[Net208] Meister, A.: "Vorratsdatenspeicherung: Details und offene Fragen", Netzpolitik.org, 19. August 2008, http://netzpolitik.org/2008/vorratsdatenspeicherung-details-und-offene-fragen/.

[OLGF08] Oberlandesgericht Frankfurt am Main: "Az 11 U 52/07", Medien Internet und Recht, Frankfurt am Main, 01. Juli 2008, http://medien-internet-und-recht.de/pdf/VT_MIR_2008_206.pdf.

[ScSc08] Schröder, B. / Schröder, C.: "Die Online-Durchsuchung", Heise Zeitschriften Verlag, Hannover, 2008, ISBN: 978-3936931532.

[Ster07] Stern.de: "Geheimdienste spitzeln schon seit Jahren", Stern.de, 25. April 2007, http://www.stern.de/computer-technik/internet/:Online-Durchsuchungen-Geheimdienste-Jahren/587865.html.

[§AdV94] Bundesministerium der Justiz: "Aufgaben der Verfassungsschutzbehörden", juris.de, 20. April 1994, http://bundesrecht.juris.de/bverfschg/__3.html.

[§BDS06] dejure.org Rechtsinformationssysteme GmbH: "Bundesdatenschutzgesetz", Mannheim, 22. August 2006, http://dejure.org/gesetze/BDSG.

[§BGB08] Bundesministerium der Justiz: "Bürgerliches Gesetzbuch", juris.de, 16. Dezember 2008, http://www.gesetze-im-internet.de/bgb/.

[§BKA08] Bundesgesetzblatt: "Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt", Bundesanzeiger Verlag, 25. Dezember 2008, Ausgabe: Teil I Nr. 66, Seiten: 3038 ff., http://www.bgblportal.de/BGBL/bgbl1f/bgbl108s3083.pdf.

[§PAG08] Bayerische Staatsregierung: "Gesetz über die Aufgaben und Befugnisse der Bayerischen Staatlichen Polizei - Artikel 34d", Bayerische Staatsregierung, 22. Juli 2008, http://www.verwaltung.bayern.de/Titelsuche-.116.htm?purl=http%3A%2F%2Fby.juris.de%2Fby%2FPolAufgG_BY_1990_Art34d.htm.

[§StG08] Bundesministerium der Justiz: "Strafgesetzbuch", juris.de, 05. November 2008, http://bundesrecht.juris.de/stgb/.

[§TKG07] dejure.org Rechtsinformationssysteme GmbH: "Telekommunikationsgesetz", Mannheim, 25. Dezember 2008, http://dejure.org/gesetze/TKG.

[§TKÜ07] Bundesgesetzblatt: "Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG", Bundesanzeiger Verlag, Köln, 31. Dezember 2007, Ausgabe: Teil I Nr. 70, Seiten: 3198 ff., http://www.bgblportal.de/BGBL/bgbl1f/bgbl107s3198.pdf.

[§TMG07] Bundesministerium der Justiz: "Telemediengesetz", juris.de, 01. März 2007, http://www.gesetze-im-internet.de/tmg/.

[§VDS06] Amtsblatt der Europäischen Union: "Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG", Amt für amtliche Veröffentlichungen der Europäischen Gemeinschaften, Luxemburg, 15. März 2006, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:DE:PDF.

[§VSG06] Innenministerium Nordrhein-Westfalen: "Gesetz über den Verfassungsschutz in Nordrhein-Westfalen", Düsseldorf, 30. Dezember 2006, http://www.im.nrw.de/sch/doks/vs/vsg_nrw_2007.pdf.

Lizenz