Humboldt-Universität zu Berlin

Institut für Informatik
Informatik in Bildung und Gesellschaft

Seminararbeit zum Thema:
Überwachung, Vorratsdatenspeicherung, Bundestrojaner, Computergrundrecht

vorgelegt von
Swetlana Klaus
(Matrikel-Nr. 185897)
und
Andreas Grüner
(Matrikel-Nr. 521149)

Berlin, 30. September 2009

Inhaltsverzeichnis

1 Einleitung

In zeitlich unregelmäßigen Abständen tritt wiederholt die politische Diskussion über die teilweise konkurrierenden Ziele der Gewährleistung der Sicherheit der Bürger und die Sicherung grundlegender Freiheiten der Staatsangehörigen auf. Diese Auseinandersetzung wird durch immer neue Forderungen im Bereich der Überwachungs– und Strafverfolgungsmaßnahmen der Innenminister, speziell des Bundesinnenminister Wolfgang Schäuble, und der Polizei entfacht. Brisante Themen in dieser Domäne sind die Ausdehnung der Telekommunikationsüberwachung, die Implementierung der Vorratsdatenspeicherung sowie der Aufbau von Know–How zur Online–Durchsuchung mit Hilfe des sogenannten Bundestrojaner. Der genannte Themenkreis spielt eine ganz besondere Rolle in der heutigen Zeit. Durch moderne Telekommunikationsmittel können Personen zu jeder Zeit auf vielen unterschiedlichen Wegen miteinander interagieren. Beispielhaft sind die Mobiltelefonie, Email–Verkehr, Chat– und Instantmessaging–Programme sowie soziale Netzwerke zu nennen. Diese Kommunikationswege werden zweifelsohne nicht nur für den privaten Gedankenaustausch sondern auch zur Vorbereitung und Koordination von Straftaten aller Arten genutzt. Dadurch entsteht ein Interesse seitens der Strafverfolgungsbehörden auf die Kommunikationsdaten Zugriff zunehmen. Dies ist innerhalb eines Rechtsstaats nur aufgrund von rechtlichen Normen, die von der Legislative verabschiedet wurden, zulässig.

In dieser Arbeit werden die zuvor genannten Themenbereiche näher erläutert und zugehörige gesetzliche Normen vorgestellt. Zu Beginn steht eine Einführung in die Grundrechte, da die Fundamentalrechte die Bürger vor staatlichen Eingriffen schützen sollen und somit den Überwachungsvorschriften entgegen stehen. Anschließend erfolgt eine Abgrenzung verschiedener Begrif-

fe mit dem Bezug zu den erfassten Daten. Im Anschluss wird der Artikel 10 Grundgesetz und in ihn eingreifende Normen sowie der Themenbereich der Vorratsdatenspeicherung vorgestellt. Das nächste Kapitel beschäftigt sich mit dem Bundestrojaner und erläutert das sogenannte Computergrundrecht. Abschließend wird in einer zusammenfassenden Betrachtung ein Überblick über die behandelten Themen gegeben.

2 Grundrechte

2.1 Bedeutung der Grundrechte

Die im Grundgesetz verankerten Fundamentalrechte besitzen eine überragende Bedeutung für die Existenz eines demokratischen Rechtsstaats. Dies ist auch an der Position der Grundrechte im Grundgesetz ersichtlich. Sie bilden den ersten Teil des Grundgesetzes und stehen direkt nach der Präambel. Einerseits findet dadurch eine klare Abgrenzung zu den im Prinzip nur zur Makulatur bestandenen Grundrechten zur Zeit des Nationalsozialismus statt und andererseits existiert eine Herausstellung der Grundrechte.

2.2 Grundrechtsfunktionen

Die Grundrechte besitzen verschiedene Funktionen, durch die sie ihre Relevanz gewinnen. Als erstes ist die Leistungsfunktion zu nennen. Dabei wird zwischen dem originären und dem derivativen Leistungsrecht unterschieden. Das originäre Leistungsrecht beschreibt die Errichtung neuer Leistungen für den Staatsbürger und ist nicht vom Grundgesetz abgedeckt. Im Gegensatz dazu charakterisiert das derivative Leistungsrecht den Anspruch an bestimmten Leistungen, welche schon existieren, teilnehmen zu dürfen.[1]

Des Weiteren stellen die Grundrechte eine Einrichtungsgarantie sowie Verfahrens– und Organisationsrecht dar und besitzen die Nichtdiskriminierungsfunktion. Die im Kontext dieser Arbeit am wichtigsten erscheinende Aufgabe expliziter Fundamentalrechte ist die Abwehrfunktion gegenüber den staatlichen Organen. Damit soll den Bürgern eine gewisse Freiheit gegenüber dem Staat garantiert werden. Es gilt sowohl die Privatsphäre als auch die persönliche Ent-

[1] Cremer, S. 363 f.

wicklung und Betätigung der Staatsangehörigen zu schützen. Dabei wird die persönliche Freiheit nicht über alles gestellt, sondern findet ihre Schranken in den Rechten anderer Personen. Die Bevölkerung steht somit dem Staat nicht wehrlos gegenüber, sondern besitzt durch die Grundrechte die Möglichkeit, sich unter anderem juristisch durch Überprüfung des staatlichen Handelns durch die Judikative auf verfassungsrechtliche Übereinstimmung und beispielsweise tatsächlich durch Demonstrationen auf Basis des Grundrechts auf Versammlungsfreiheit zur Wehr zu setzen.[2]

2.3 Eingriff in ein Grundrecht

Eingriffe in Grundrechte sind nicht absolut verboten, sondern unterliegen strengen Kriterien. Behauptet eine Person, dass sie in ihren Grundrechten verletzt worden sei, so beginnt eine juristische Prüfung nach folgendem Schema. An erster Stelle wird der Schutzbereich des angeblich verletzten Grundrechts geprüft. Danach erfolgt die Untersuchung ob das Grundrecht in vorliegender Weise eingeschränkt werden darf und im Anschluss daran muss geklärt werden, ob bestimmte Schranken der angewandten Beschränkung außer Acht gelassen worden sind.[3]

Schutzbereich

Die Untersuchung des Schutzbereiches eines Grundrechts gliedert sich in drei Stufen: Die persönliche, die örtliche und die sachliche Ebene.[4] Beginnend bei dem persönlichen Schutzbereich findet eine Überprüfung statt, ob sich die Person, welche die Grundrechtsverletzung geltend macht, auf das vorgetragene

[2] Bultmann, S. 175 f.
[3] Katz, S. 316 f.
[4] Bultmann, S. 175 f.

Grundrecht berufen kann. Dabei erfolgt eine Einteilung der Grundrechte einerseits in Menschenrechte und andererseits in die Bürgerrechte. Ein Menschenrecht ist beispielsweise Artikel 1 Grundgesetz: "Die Würde des Menschen ist unantastbar. "Innerhalb dieser Kategorie der Grundrechte ist der persönliche Schutzbereich für alle Menschen eröffnet, treffend durch den Begriff "Jedermannsrechte "umschrieben. Die Bürgerrechte gelten dagegen nur für deutsche Staatsangehörige. Ein Beispiel für ein Bürgerrecht ist Artikel 8 Grundgesetz: "Alle Deutschen haben das Recht, sich ohne Anmeldung und Erlaubnis friedlich und ohne Waffen zu versammeln."Seit der Unterzeichnung des EG–Vertrages durch Deutschland sind bei den Bürgerrechten unter dem Begriff der Deutschen alle EU–Staatsangehörigen zusammenzufassen. Dies geht aus dem Nichtdiskriminierungsverbot des Artikel 10 des EG–Vertrages hervor.[5]

Die nächste zu überprüfende Materie ist der örtliche Komplex. Der örtliche Schutzbereich eines Grundrechts ist als eröffnet anzusehen, falls der grundrechtsverletzende Vorfall auf dem Hoheitsgebiet der Bundesrepublik Deutschland stattfindet. Zu diesem Areal gehört das Gebiet in den geografischen Grenzen von Deutschland. Hinzu kommen die Vertretungen der Bundesrepublik im Ausland sowie der Bundeswehr unterstehende Stützpunkte außerhalb Deutschlands.

Am Ende der Schutzbereichsprüfung wird die sachliche Ebene untersucht. Sie dient der Klärung, ob der stattgefundene Sachverhalt beziehungsweise die ausgeübte Tätigkeit des Bürgers unter ein bestimmtes Grundrecht subsumiert werden kann. Dazu wird der entsprechende Artikel mit dem Fundamentalrecht analysiert. Dabei erfahren unbestimmte Begriffe eine Definition. Anschließend

[5]EGV, EG–Vertrag (Vertrag zur Gründung der Europäischen Gemeinschaft). In der Fassung vom 02.10.1997. Zuletzt geändert durch den Vertrag über den Beitritt der Republik Bulgarien und Rumäniens zur Europäischen Union vom 25.4.2005 (ABl. EG Nr. L 157/11) m.W.v. 1.1.2007.

wird das Geschehen mit der sachlichen Lage des Artikels verglichen. Werden alle drei Ebenen des Schutzbereiches eines Grundrechts eröffnet, so genießt die handelnde Person den besonderen Schutz des geprüften Fundamentalrechts.

Schranken

Das durch eine Person maßlose Ausüben und Nutzen der durch die Grundrechte gewährten Freiheiten kann zu einer Grundrechtsverletzung eines anderen Bürgers führen oder den gesellschaftlichen Frieden stören. Deshalb besteht die Möglichkeit die Fundamentalrechte in bestimmter Weise einzuschränken. Somit existiert eine Legitimationsgrundlage staatlichen Handelns zum Eingriff in die Grundrechte. Es werden diverse Typen von Schranken unterschieden.

Eine erste Möglichkeit, in der ein Grundrecht seine Grenzen findet, sind die verfassungsimmanenten Schranken. In diesem Bereich wird von konkurrierendem Verfassungsrecht gesprochen, d. h. Grundrechte finden ihre Schranken in den anderen Grundrechten. Es muss ein Abwägungsprozess erfolgen, bei dem ermittelt wird, in wie weit welches Fundamentalrecht in ein anderes hineingreift und welchem in der speziellen Situation der Vorrang einzuräumen ist.[6]

Eine weitere Schrankenart sind die sogenannten verfassungsunmittelbaren Schranken. Innerhalb dieses Kontext werden die Rechte und Freiheiten, die die sprachliche Ausgestaltung des Fundamentalrechts den Bürgern einräumt durch den weiterfolgenden Wortlaut wieder im begrenzten Maße eingeschränkt.[7] Ein Beispiel für diese Form der Beschränkung ist in Artikel 2 Absatz 1 des Grundgesetzes zu finden: “Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.”

[6]Katz, S. 209 f.
[7]Katz, S. 308.

Die dritte und abschließende Form der Beschränkungsmöglichkeiten ist der Gesetzesvorbehalt. Hierbei geht es um die Einschränkung eines Grundrechts aufgrund von Gesetzen. Damit dies geschehen darf steht eine Erlaubnis im Fundamentalrechtsartikel im Grundgesetz.[8] Als Beispiel ist Artikel 8 Absatz 2 zu nennen: "Für Versammlungen unter freiem Himmel kann dieses Recht durch Gesetz oder auf Grund eines Gesetzes beschränkt werden. "Dem beschränkenden Gesetz sind formelle Hürden aufgelegt. Es muss das Zitiergebot –das eingeschränkte Grundrecht muss im Gesetz explizit genannt werden –und die Wesensgehaltsgarantie beachtet werden. Die Wesensgehaltsgarantie umschreibt, dass der Kern des Grundrechts nicht angetastet werden darf und das rationierte Recht im Wesen für den Bürger weiter ausübbar ist.[9]

Schranken – Schranken

Ist der Schutzbereich des Grundrechts eröffnet, und besitzt das intervenierende staatliche Organ eine formell und materiell rechtmäßige Ermächtigungsgrundlage basierend auf den Einschränkungsmöglichkeiten aus dem vorherigen Abschnitt, so kann die Legitimität des Grundrechtseingriffs durch Nichtbeachtung der Schranken–Schranken weiterhin nicht gegeben sein. Schranken–Schranken in diesem Sinne sind juristische Regelungen, die die Eingriffsgrundlage der Exekutivorgane limitiert. Dies können einerseits einfach gesetzliche Regelungen sein, welche dem Staat bestimmte Auflagen zur Durchführung eines Eingriffs oktroyieren und andererseits gesetzesübergreifende Prinzipien, wie unter anderem der Verhältnismäßigkeitsgrundsatz, der bei jeglichem staatlichen Handeln durch die ausführenden Organe beachtet werden muss.[10]

[8] Katz, S. 308 f.
[9] Duden, Wesensgehaltsgarantie.
[10] Katz, S. 102.

Die Prüfung des Verhältnismäßigkeitsgrundsatzes besteht aus drei Phasen: die Untersuchung der Geeignetheit, Erforderlichkeit und Angemessenheit. Bei der Geeignetheit wird der Frage nachgegangen, ob mit dem gewählten Eingriffsmittel auch wirklich das erwünschte Ziel erreicht werden kann oder ob der Einsatz ergebnislos verlaufen würde und somit der Grundrechtseingriff nicht stattfinden müsste. Im Bereich der Erforderlichkeit erfolgt die Untersuchung des gewählten Mittels auf seine Eingriffsintensität. Es wird geprüft ob das mildeste Instrument verwendet wurde. Ein praxisnahes Beispiel zu dieser Frage ist die Beschlagnahmung von Computern bei Hausdurchsuchungen. Es besteht die Möglichkeit, die ganze IT–Hardware als Beweismittel zu konfiszieren oder die Datenträger zu kopieren. Hier ist eindeutig der Kopiervorgang das mildere Mittel, da die betroffene Person ihre IT–Geräte weiterverwenden kann im Gegensatz zur kompletten Beschlagnahmung. Abschließend wird die Angemessenheit der Maßnahme geprüft. Die Abwägung verschiedener Güter erfolgt in diesem Abschnitt. Auf der einen Seite steht das zu schützende Grundrecht und ihm gegenüber gestellt befindet sich ein anderes Gut. Bei der Aufklärung von Straftaten ist dies zum Beispiel die öffentliche Ordnung und Sicherheit oder die Belangung des Straftäters.[11]

[11] Katz, S. 102 ff.

3 Datenarten

Im Bereich der Überwachung von Telekommunikations– und Informationstechniksystemen treten verschiedene Begriffe über die diversen kontrollierten und gespeicherten Daten auf. Um in den nachfolgenden Kapiteln eine gemeinsame Verständnisgrundlage zu haben besonders in Hinblick auf den sachlichen Schutzbereich des Artikel 10 Grundgesetz, sollen diese im aktuellen Abschnitt erklärt werden.

Inhaltsdaten

Unter dem Begriff der Inhaltsdaten werden "Nachrichten oder Informationen, die mittels Telekommunikation ausgetauscht werden "[12] verstanden. Als Beispiel wäre der Text einer SMS oder die übermittelten Informationen in einer E–Mail zu nennen.

Bestandsdaten

Der Fachterminus Bestandsdaten umfasst die "Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden. "[13] Dies sind beispielsweise die Vor– und Zunamen des Telekommunikationsteilnehmers, die postalische Adresse sowie die Bankverbindung zur Begleichung der entsprechenden Rechnungen.

[12] Keller, S. 13 f.
[13] Keller, S. 14.

Verkehrsdaten

"Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben verarbeitet oder genutzt werden "[14] sind unter dem Ausdruck Verkehrsdaten zu subsumieren. Nach § 96 Abs. 1 Telekommunikationsgesetz[15] fallen unter anderem in den Bereich der Verkehrsdaten die Nummer und die Kennung der Anschlüsse, Beginn und Ende der Verbindung sowie den vom Nutzer in Anspruch genommenen Telekommunikationsdienst.

Standortdaten

Standortdaten werden als "Daten, die in einem Telekommunikationsnetz erhoben oder verwendet werden und die den Standort des Endgeräts eines Endnutzers eines Telekommunikationsdienstes für die Öffentlichkeit angeben "[16] definiert. Standortdaten werden als Teilmenge der Verkehrsdaten angesehen.

[14] Keller, S. 14 f.

[15] TKG, Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch Artikel 2 des Gesetzes vom 14. August 2009 (BGBl. I S. 2821) geändert worden ist.

[16] Keller, S. 15.

4 Artikel 10 Grundgesetz

Der Artikel 10 des Grundgesetzes schützt maßgeblich die Vertraulichkeit privater Kommunikation sowohl auf analogem als auch digitalem Wege. Dadurch ergibt sich eine entscheidende Relevanz für den Bereich der Telekommunikationsüberwachung. In diesem Kapitel wird der Schutzbereich des Art. 10 GG erörtert.

4.1 Sachlicher Schutzbereich

Im ersten Absatz des Artikel 10 Grundgesetz wird das Brief– , Post und Fernmeldegeheimnis für unverletzlich erklärt. Das Briefgeheimnis bewahrt die Vertraulichkeit bei der Übermittlung von Sendungen durch die Post. Vor dem Öffnen durch staatliche Organe sind alle Sendungen wie Pakete und Briefe geschützt. Es herrscht aber ein Diskurs in der einschlägigen Literatur und das Auseinander gehen von Fachmeinungen im Bezug auf die Postkarte. Der herrschenden Meinung nach wird die Wertigkeit des Schutzes einer Postkarte einem ungeöffneten Brief oder Paket gleich gestellt.[17] Bei einer Minderheit dagegen wird die Postkarte als nicht schützenswert betrachtet, oder es wird in nur einem geringerem Umfang gegenüber dem Brief die Vertraulichkeit der Postkarte als achtenswert eingeschätzt.[18] Als Begründung für die zweite Sichtweise dient die Öffentlichkeit der übermittelten Nachricht. Der Informationstext für den Empfänger steht für jeden, aber besonders für die Angestellten des Postdienstleisters gut sicht– und lesbar auf der Rückseite der Karte. Deshalb muss der Absender davon ausgehen, dass die Karte gelesen wird und er ist sich dadurch selbst, schon während des Schreib– und Absendevorgangs der Karte, im Klaren, dass

[17] Hesselberger, S. 139.
[18] LG Köln, Urteil vom 06.09.2006, Az. 280178/06.

er vertrauliche Nachrichten auf diesem Wege nicht diskret übermitteln kann.

Ein weiteres Element des Schutzbereiches ist das Postgeheimnis. Das Postgeheimnis umfasst alle Dienstleistungen und ausgeführten Arbeiten, die im Zusammenhang mit der Beförderung von Briefen, Paketen und anderen Sendungen stehen. Dies betrifft unter anderem die Adresse von Absender und Empfänger.[19]

Der letzte durch den Artikel 10 des Grundgesetzes geschützter Bereich ist das Fernmeldegeheimnis. In diesen Komplex fällt die Übertragung immatrieller Informationen mit technischen Methoden des Fernmeldeverkehrs.[20] Sowohl kabelgebundene als auch kabellose Übertragungsverfahren werden unter diese Sektion subsumiert.

Im Allgemeinen ist der Schutzbereich des Artikel 10 Grundgesetz für Inhalts– und Verkehrsdaten im Brief– , Post– und Fernmeldegeheimnis eröffnet.

4.2 Persönlicher Schutzbereich

Der Artikel 10. Grundgesetz ist ein Jedermannsrecht und somit ist der persönliche Schutzbereich für alle Menschen gegenüber dem deutschen Staat eröffnet.[21]

4.3 Örtlicher Schutzbereich

Der örtliche Schutzbereich ist nicht grundrechtsspezifisch und immer auf deutschem Hoheitsgebiet eröffnet. Genauere Ausführungen sind im Kapitel 2 Abschnitt 3 vorzufinden.

[19] Hesselberger, S. 139.
[20] Hesselberger, S. 139.
[21] Groepl, 1. Schutzbereich.

5 Telekommunikationsüberwachung

Im Abschnitt “Eingriff in ein Grundrecht ”wurde beschrieben, welche Hürden es gibt, damit in ein Fundamentalrecht eingegriffen werden kann. Im Absatz 2 des Artikel 10 Grundgesetz sind Beschränkungen aufgrund von Gesetzen erlaubt. Im Nachfolgenden werden die Eingriffsnormen der Strafprozessordnung und des Gesetzes zur Beschränkung des Brief– , Post– und Fernmeldegeheimnisses mit dem Augenmerk auf dem Fernmeldeverkehr betrachtet.

5.1 Normen der Strafprozessordnung

In der Strafprozessordnung sind im Hinblick auf die Telekommunikationsüberwachung folgende Normen von Belang. Im § 100a der Strafprozessordnung (StPO)[22] werden die Voraussetzungen für die Anordnung einer Telekommunikationsüberwachungsmaßnahme definiert. Modalitäten der Anordnung und Durchführung eines solchen Vorgehens werden in § 100b StPO geregelt. Im Rahmen der Telekommunikationsüberwachung werden Inhaltsdaten erhoben. In § 100g der Strafprozessordnung wird die Erhebung von Verkehrsdaten geregelt. Nachstehend werden die einzelnen Normen näher erläutert.

§100a StPO

Der § 100a StPO gliedert sich in vier Absätze und nennt die matriellen Voraussetzungen für die Telekommunikationsüberwachung. Im ersten Absatz wird die grundlegende Eingriffsnorm beschrieben. Nach § 100a I StPO darf die Telekommunikation einer Person auch ohne ihres Wissens erfolgen, wenn bestimmte

[22] StPO, Strafprozeßordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 3 des Gesetzes vom 30. Juli 2009 (BGBl. I S. 2437) geändert worden ist.

Tatbestände vorliegen. Es müssen Anhaltspunkte vorliegen, dass das Individuum eine schwere Straftat vorbereitet, versucht oder schon begangen hat. Des Weiteren muss diese Tat im Einzelfall schwerwiegen und die Untersuchung der Situation mit anderen Maßnahmen nicht Erfolg versprechend sein. Die Straftaten, bei denen eine Telekommunikationsüberwachung angeordnet werden kann, sind in § 100a II StPO geregelt. Darunter befinden sich Delikte aus dem Strafgesetzbuch, der Abgabenordnung, dem Arzneimittelgesetz, dem Aufenthaltsgesetz, dem Betäubungsmittelgesetz, dem Völkerstrafgesetzbuch, dem Waffengesetz und weiteren Gesetzbüchern. Das interessanteste und bedeutendste Gesetz in diesem Bereich ist das Strafgesetzbuch (StGB)[23]. Im Folgenden wird ein Auszug der Straftaten genannt, die der Polizei den Einsatz der Telekommunikationsüberwachung ermöglichen. Dies sind unter anderem Hochverrat, Geldfälschung, Mord, Raub, Erpressung und Computerbetrug. Das Delikt Computerbetrug wird in § 263a StGB geregelt und umfasst die Verschaffung eines rechtswidrigen vermögenswerten Vorteils unter der unbefugten oder unvollständigen Benutzung von Daten oder die Nutzung bestimmter Programme. Es ist nach § 263a II StGB auch strafbar, solche Programme für das Ziel eines Computerbetrugs herzustellen. In den Absätzen drei und vier des § 100a StPO werden zusätzliche Einschränkungen zum Einsatz der Telekommunikationsüberwachung getroffen. Einerseits darf sie sich nur gegen die Person richten, die dem Delikt aus dem Straftatenkatalog beschuldigt wird, oder eine Person, der die Kommunikation des Beschuldigten übernimmt. Des Weiteren dürfen keine Informationen aus dem sogenannten Kernbereich privater Lebensgestaltung aufgezeichnet und verwertet werden. Ist eine Aufzeichnung geschehen, müssen die erlangten Daten umgehend gelöscht werden.

[23]StGB, Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), das zuletzt durch Artikel 3 des Gesetzes vom 2. Oktober 2009 (BGBl. I S. 3214) geändert worden ist.

§100b StPO

Der § 100b StPO umfasst sechs Absätze und regelt die formellen Voraussetzungen für die Anordnung und Durchführung der Maßnahme der Telekommunikationsüberwachung. Im ersten Absatz dieser Norm ist der Richtervorbehalt geregelt. Eine Telekommunikationsüberwachung darf nur von einem Richter angeordnet werden. Bei Gefahr im Verzug ist dazu auch die Staatsanwaltschaft befugt. Danach muss innerhalb von drei Tagen die Anordnung von einem Gericht bestätigt werden. Im zweiten Passus dieses Paragraphen werden die Bestandteile und die Form einer Anordnung festgelegt. Sie muss immer schriftlich erfolgen. Es ist der Name und die Adresse des zu Überwachenden zu nennen. Zudem muss eine Identifikation des Kommunikationsmittel des Betroffenen erfolgen. Außerdem ist die Dauer mit exakt genannten Endzeitpunkt der Überwachungsmaßnahme eine Komponente der Anordnung zur Telekommunikationsüberwachung. In den weiteren Abschnitten werden die Folgen bei Wegfall der Voraussetzungen der Anordnung abgehandelt und eine Berichtspflicht der Staatsanwaltschaften gegenüber dem Bundesjustizministerium über durchgeführte Überwachungsmaßnahmen eingeführt.

§100g StPO

Der § 100g StPO regelt die Erhebung von Verkehrsdaten innerhalb von vier Abschnitten. Die materiellen Voraussetzungen für die Erhebung von Verkehrsdaten in § 100g I StPO sind analog zu den Prämissen für die Erfassung von Inhaltsdaten gemäß § 100a I StPO. Es wird in diesem Paragraph derselbe Straftatenkatalog referenziert.

5.2 Normen des Gesetzes zur Beschränkung des Brief– Post und Fernmeldegeheimnisses

Aus dem Gesetz zur Beschränkung des Brief– , Post und Fernmeldegeheimnis (G10)[24] werden nachstehend folgende Normen vorgestellt. In § 1 G10 wird der Gegenstand des Gesetzes beschrieben. § 2 G10 umfasst Verpflichtungen der Telekommunikationsdiensteanbieter und § 3 G10 enthält die Voraussetzungen für die Anwendung des Gesetzes.

§1 G10

Der § 1 des Gesetzes zur Beschränkung des Brief– , Post und Fernmeldegeheimnisses stellt die Eingriffsgrundlage für bestimmte Behörden zur Überwachung der Telekommunikation und der Aufhebung des Post– und Briefgeheimnis. Nach § 1 I Nr. 1 G10 werden die Verfassungsschutzbehörden, der militärische Abschirmdienst und der Bundesnachrichtendienst dazu ermächtigt, wenn unter anderem die freiheitlich demokratische Grundordnung (FDGO) Deutschlands und die Sicherheit der Länder bedroht ist. Die freiheitlich demokratische Grundordnung ist ein im Gesetz über den Bundesverfassungsschutz (BVerfSchG)[25] legaldefinierter Begriff. In § 4 II BVerfSchG werden zur FDGO unter anderem die Menschenrechte, die Unabhängigkeit der Gerichte und der Ausschluss jeglicher Gewalt und Willkürherrschaft gezählt.

[24] G10, Artikel 10–Gesetz vom 26. Juni 2001 (BGBl. I S. 1254, 2298), das zuletzt durch Artikel 1 des Gesetzes vom 31. Juli 2009 (BGBl. I S. 2499) geändert worden ist.

[25] BVerfSchG, Bundesverfassungsschutzgesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2970), das zuletzt durch Artikel 1a des Gesetzes vom 31. Juli 2009 (BGBl. I S. 2499) geändert worden ist.

§2 G10

Der § 2 G10 beinhaltet Pflichten für die Post– und Telekommunikationsdiensteanbieter. Im ersten Absatz werden die Postdienstleister verpflichtet, Sendungen und alle dafür vorhandenen Daten auf Anordnung an die anweisende staatliche Stelle herauszugeben. Des Weiteren wird für die Provider von Telekommunikationsdiensten verbindlich festgelegt, dass sie auf Anordnung Inhalte der Kommunikation aufzeichnen und der anfragenden Behörde übermitteln müssen. Im Absatz 2 wird die Notwendigkeit der einfachen Sicherheitsüberprüfung für Personen, welche die Inhalte der Kommunikation bei entsprechenden Providern aufzeichnen, festgelegt.

§3 G10

In § 3 G10 werden die Voraussetzungen für die Überwachung der Kommunikation nach § 1 G10 genannt. Einerseits muss es begründete Anzeichen für gesetzlich bestimmte Straftaten, beispielsweise Hochverrat, Landesverrat oder Straftaten gegen die Sicherheit Deutschlands, geben und andererseits muss die Aufklärung durch Nichteinsatz der Mittel des Gesetzes zur Beschränkung des Brief– , Post und Fernmeldegeheimnisses bedeutend erschwert sein.

6 Vorratsdatenspeicherung

6.1 Sachverhalt

Der Ausgang der Vorratsdatenspeicherung ist die EG–Richtlinie 2006/24/EG[26] des europäischen Parlaments und des europäischen Rates. In dieser Richtlinie wird den Telekommunikationsprovidern die Speicherung von Verkehrs–und Standortdaten für die Bereiche Telefonie, Internet–Access und E–Mail im Bereich der Mitgliedsländer der europäischen Union auferlegt. Die Speicherdauer soll einen Zeitraum von mindestens sechs Monate bis maximal zwei Jahre betragen. Die Umsetzung dieser europäischen Richtlinie erfolgte mit der Änderung des Telekommunikationsgesetzes[27]. Damit ist diese Normensammlung entscheidend für die Vorratsdatenspeicherung und wird im nachfolgenden Abschnitt behandelt.[28]

6.2 Telekommunikationsgesetz

Der entscheidende Paragraph des Telekommunikationsgesetzes (TKG) für die Vorratsdatenspeicherung ist die Bestimmung des § 113a TKG. Zusätzlich wird im § 113b TKG die Verwendung der gespeicherten Verkehrs– und Standortdaten geregelt.

[26] 2006/24/EG, 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.

[27] TKGuaÄndG, Artikel 2 des Gesetzes vom 14. August 2009 (BGBl. I S. 2821).

[28] Keller, S.37 f.

§113a TKG

In § 113a I TKG wird der Begriff der Telekommunikationsdiensteanbieter definiert. Es sind Einrichtungen, die öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringen. Gleichzeitig werden diese verpflichtet, die Verkehrsdaten zu speichern. Im zweiten Absatz dieses Paragraphen werden die zu speichernden Daten für Telefonieprovider näher charakterisiert. Es muss unter anderem folgendes gespeichert werden: die Kennung der Telefonanschlüsse, der Beginn und das Ende der Verbindung sowie bei Mobilfunkverbindungen die Funkzelle bei Eröffnung der Kommunikation. Durch § 113a III TKG werden die zu speichernden Daten für E–Mail Anbieter geregelt. Es müssen bei Versenden und Eingang der elektronischen Nachricht die Kennung der Postfächer, die IP–Adressen sowie die Zeitpunkte gespeichert werden. Zusätzlich muss die Zeit sowie die IP–Adresse und das Postfach des Empfängers bei Abholung der E–Mail gespeichert werden. Abschließend werden in § 113a IV TKG die Verkehrsdaten im Bereich Internet–Access geregelt. Hier müssen Anfang und Ende sowie IP–Adresse des Verbindungsnehmers festgehalten werden. Nach § 113a VIII TKG wird verboten, den Inhalt der Kommunikation zu speichern.

§113b TKG

Nach § 113b TKG dürfen die aufgrund des § 113a TKG gespeicherten Daten nur für bestimmte Zwecke Verwendung finden. Darunter fällt die Verfolgung von Straftaten, die Abwehr von Gefahren für die öffentliche Sicherheit und die Ausübung der gesetzlich vorgeschriebenen Aufgaben der Verfassungsschutzbehörden, des Bundesnachrichtendienstes sowie der des militärischen Abschirmdienstes.

6.3 Verfassungsmäßigkeit der Vorratsdatenspeicherung

Die Verfassungsmäßigkeit der Vorratsdatenspeicherung ist bis zum heutigen Zeitpunkt noch ungeklärt. Eine Verfassungsbeschwerde beim Bundesverfassungsgericht ist anhängig. Das Bundesverfassungsgericht erließ seit dem Einreichen der Beschwerde mehrere befristete einstweilige Verfügungen zur Beschränkung der Herausgabe der gespeicherten Verkehrs–und Standortdaten.[29]

Die wichtigsten Gründe, die von den Beschwerdeführern der Klage gegen die Vorratsdatenspeicherung angeführt werden, werden im Folgenden betrachtet. Die Vorratsdatenspeicherung wird als unverhältnismäßig angesehen. Der Verhältnismäßgkeitsgrundsatz besteht aus den Prüfpunkten Geeignetheit, Erforderlichkeit und Angemessenheit (siehe Abschnitt "Schranken–Schranken", im Kapitel Grundrechte). Die Vorratsdatenspeicherung könnte den Grundsatz der Erforderlichkeit verletzen, da ein milderes Mittel existiert: Das Quick–Freeze–Verfahren. Bei dieser Methode setzen sich die staatlichen Stellen mit dem Telekommunikationsdiensteanbieter in Verbindung und verlangen die Speicherung der Verkehrs– und Standortdaten. Der Provider speichert diese und überträgt sie erst an die staatlichen Stellen, wenn ein Gericht über die Zulässigkeit der Speicherung entschieden hat. Dadurch gehen im Rahmen von Verzögerungen keine Daten verloren und es kann trotzdem eine unabhängige Nachprüfung der Rechtmäßigkeit erfolgen. Weitere Gründe sind das Stellen der Bevölkerung unter einen Generalverdacht und formelle sowie materielle Mängel in der Rechtmäßigkeit der ausgehenden EG–Richtlinie.[30]

[29] Vorratsdatenspeicherung, Sammel–Verfassungsbeschwerde gegen Vorratsdatenspeicherung.

[30] Keller, S. 40 f.

7 Online–Durchsuchung/Computergrundrecht

Seit dem 01.01.2009 ist das "Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt" vom 25.12.2008 in Kraft.[31] Es gestattet dem BKA unter anderem die heimliche Online–Durchsuchung von Computern und anderen IT–Systemen zur frühzeitigen Gefahrenerkennung durchzuführen, um an tatsächlich oder vermeintlich sicherheitsrelevante Informationen zu gelangen.

Potentiell betroffen sind alle, die einen Computer mit Internetanschluss besitzen. Ein heimlicher Zugriff gewährt den staatlichen Stellen Zugang zu einem Datenbestand, der detaillierte Informationen über persönliche Beziehungen, die Lebensgestaltung, die Kommunikationswege und –partner sowie auch höchst persönliche Aufzeichnungen (z.B. Tagebücher) erfassen könnte. Die erhobenen Daten ermöglichen weitreichende Rückschlüsse auf die Persönlichkeit des Betroffenen bis hin zum Erstellen von Verhaltens– und Kommunikationsprofilen.[32] Damit handelt es sich bei der Online–Durchsuchung um eine Maßnahme, die mit einem erheblichen Eingriff in Grundrechte des Betroffenen verbunden ist.

Das Bundesverfassungsgericht hat deswegen in seiner Rechtssprechung strenge Anforderungen an die Durchführung solcher Maßnahmen gestellt und zudem das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme entwickelt.[33] Dieses neue IT–Grundrecht als Ausprägung des allgemeinen Persönlichkeitsrechts schützt vor Eingriffen in informationstechnische Systeme, soweit der Schutz nicht durch andere Grundrechte gewährleistet ist.[34]

[31] BGBl. I, S. 3083.
[32] BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz–Nr. 229 ff.
[33] BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz–Nr. 166 ff.
[34] BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz–Nr. 167.

Im Rahmen dieser Seminararbeit sollen die einzelnen Gesichtspunkte der Online–Durchsuchung näher erläutert werden. Zunächst wird ein Überblick über die verwendeten Begriffe gegeben und die rechtliche Grundlage dargestellt. Dabei wird das neue Computer–Grundrecht sowie die Umsetzung im BKA–Gesetz im Detail betrachtet. Abschließend werden Erforderlichkeit und Beweiskraft dieser Maßnahme diskutiert und weitere Kritikpunkte angesprochen.

7.1 Definition der Begriffe

Die Änderung des Verfassungsschutzgesetzes des Landes Nordrhein–Westfalen im Jahre 2006 hat heftige Diskussionen in Bezug auf die Online–Durchsuchung ausgelöst. Das Gesetz erlaubte den heimlichen Zugriff auf informationstechnische Systeme durch Einsatz technischer Mittel. Sowohl in der Politik als auch in den Medien gab es zahlreiche Auseinandersetzungen mit dem Thema. Im Rahmen dieser Diskussionen sind viele Bezeichnungen entstanden. Die verwendeten Begriffe sind aber meist irreführend und sollen deshalb hier erläutert werden.

Informationstechnisches System

Ein informationstechnisches System ist eine Einheit aus Hard–, Software und Daten, die der Erfassung, Speicherung, Verarbeitung, Übertragung und Anzeige von Informationen und Daten dient. Es sind also nicht nur Personalcomputer, Laptops oder Server gemeint, sondern auch das Internet in der Gesamtheit, Rechnernetzwerke, Telekommunikationsgeräte, PDAs, SmartPhones, MP3–Player, elektronische Terminkalender, verschiedene elektronische Geräte in Wohnungen und Kraftfahrzeugen, usw.[35]

[35]BMI Fragenkatalog des Bundesministeriums der Justiz, S. 2-5.

Online–Durchsuchung

Unter Online–Durchsuchung versteht man den heimlichen Zugriff staatlicher Stellen mittels technischer Mittel auf informationstechnische Systeme über Kommunikationsnetze. Der Begriff umfasst sowohl die einmalige Durchsuchung eines IT–Systems – die sogenannte Online–Durchsicht – als auch eine sich über einen längeren Zeitraum erstreckende Überwachung, die Online–Überwachung. Außer in der Dauer unterscheiden sich diese zwei Maßnahmen lediglich in Bezug auf den Zweck.

Bei der Online–Durchsicht soll der momentane Zustand ermittelt werden: "Was hat die Zielperson bezogen auf ihr IT–System in der Vergangenheit gemacht?" Es sollen zum einen Informationen über das System selbst erhoben werden, zum anderen über die auf dem Zielsystem gespeicherte Daten. Dabei kann zum Beispiel nach Dateien mit bestimmten Namen oder Dateiendungen, in bestimmten Verzeichnissen oder nach bstimmten Schlüsselworten gesucht werden.

Bei der Online–Überwachung dagegen sollen über einen gesetzlich festgelegten Zeitraum die Aktivitäten des Nutzers protokolliert werden: "Was macht die verdächtige Person bezogen auf ihr IT–System aktuell?" Es werden zusätzlich flüchtige Daten erfasst, wie beispielsweise Passwörter, Texte, die nicht übertragen werden, sowie Klartexte vor der Verschlüsselung beziehungsweise nach der Entschlüsselung. Weiterhin können Keylogger zum Abfangen von Tastatureingaben eingesetzt werden.[36]

[36]BMI Fragenkatalog des Bundesministeriums der Justiz, S. 6.

Quellen–Telekommunikationsüberwachung

Telekommunikationsinhalte sollten nicht Gegenstand der Online–Überwachung sein, hier gelten die ursprünglichen Regelungen zur Telekommunikationsüberwachung. Die Quellen–TKÜ dient ausschließlich der Erhebung von Kommunikationsdaten, während die Online–Durchsuchung auf die Sicherung von gespeicherten Daten abzielt. Das bedeutet, dass weder digitale Telekommunikationsgeräte Ziel der Online–Überwachung sind noch eine Belauschung von Ferngesprächen an PCs erfolgt (z.B. via Voice over IP).

Remote Forensic Software

RFS ist die interne Bezeichnung des Bundeskriminalamtes der für die Online–Durchsuchung zu verwendenden Software. Da diese Software einen heimlichen Zugriff auf IT–Systeme ermöglichen soll, zählt sie zur Kategorie der Schadsoftware und wird von Kritikern oftmals als Bundestrojaner oder Computerwanze bezeichnet.[37]

Den Vorgang, bei dem eine Durchsuchungssoftware auf dem IT–System der verdächtigen Person installiert wird, bezeichnet man als Infiltration.

7.2 Technische Umsetzungsmöglichkeiten

Die technischen Details für die Online–Durchsuchungen sind nicht bekannt. In den Antworten des BMI zu den Fragekatalogen des BMJ und der SPD–Bundestagsfraktion sowie in den Gutachten für das Bundesverfassungsgericht werden verschiedene Möglichkeiten genannt, die hier kurz vorgestellt werden.

[37] Siehe dazu http://www.heise.de/newsticker/meldung/24C3-Kampf-gegen-Schaeubles-Computerwanze-173847.html

Die Durchführung der Online–Durchsuchung umfasst die Analyse des zu durchsuchenden Systems, die Installation der Durchsuchungssoftware sowie die eigentliche Durchführung der Maßnahme.[38] Die Durchsuchungssoftware soll individuell entwickelt und auf das Zielsystem abgestimmt werden. Dazu sind diverse Angaben zur Soft– bzw. Hardware sowie Informationen zum Verhalten des Nutzers erforderlich. Die Analyse des Zielsystems kann online, durch Observation und sonstige herkömmliche Ermittlungsmethoden erfolgen.

Infiltration der Durchsuchungssoftware

Nach der Auswertung der Ergebnisse und Anpassung muss die Durchsuchungssoftware auf dem Zielsystem installiert werden. Es gibt zwei unterschiedliche Methoden: entweder erfolgt der Zugriff elektronisch über die Kommunikationsnetze oder die Software wird direkt auf dem Zielsystem installiert.[39]

a). Infiltration durch Zugriff über Kommunikationsnetze
Bei einer Installation über Kommunikationsnetze hat man die gleichen technischen Optionen wie Angreifer aus der Wirtschaftskriminalität oder Virenautoren. Man versucht über das Internet die Schadsoftware auf das Zielsystem aufzuspielen, z.B. über den Versand von E–Mails mit Anhang, durch manipulierte Webseiten oder infizierte Downloads. Dazu ist allerdings das unbewusste Mitwirken des Benutzers erforderlich. Es besteht aber auch die Möglichkeit, die vorhandenen Sicherheitslücken in bereits installierter Software auszunutzen (z.B. mit einem Zero–Day–Exploit).

[38] Fox, Stellungnahme zur "Online–Durchsuchung", S. 5.
[39] Fox, Stellungnahme zur "Online-Durchsuchung", S. 6.

b). Infiltration durch physischen Zugriff

Die Durchsuchungssoftware kann aber auch durch einen direkten physischen Zugriff auf das Zielsystem installiert werden, z.B. über ein ungesichertes WLAN, Zusenden/ Herumliegenlassen von infizierten Datenträgern oder durch heimliches Eindringen in die Räumlichkeiten, in denen sich das Zielsystem befindet.

c). Keine Infiltration

Eine weitere Möglichkeit zur Informationsgewinnung besteht in der passiven Beobachtung des IT-Systems, bei der die elektromagnetische Abstrahlung des Zielsystems oder die akustischen Signale ausgewertet werden. [40] Dabei werden nur Informationen gewonnen, die auf dem Zielsystem direkt eingegeben werden, z.B. Passwörter für verschlüsselte Daten. Diese Erkenntnisse können dann bei der offenen Beschlagnahme der IT–Systeme zur Untersuchung herangezogen werden.

Datengewinnung und Kommunikation

Der erfolgreichen Infiltration folgt die eigentliche Online–Durchsuchung des Systems, ggf. die Zwischenspeicherung und Übertragung der Daten und anschließend die Beendigung der Maßnahme mit der Benachrichtigung der Betroffenen. [41]

[40] Roggan(Hrsg.), Hansen/Pfitzmann, Techniken der Online–Durchsuchung: Gebrauch, Missbrauch, Empfehlungen, S. 134

[41] Roggan(Hrsg.), Hansen/Pfitzmann, Techniken der Online–Durchsuchung: Gebrauch, Missbrauch, Empfehlungen, S. 137-139

7.3 Rechtsgrundlage

Die ersten Online–Durchsuchungen wurden bereits im Jahre 2005 durchgeführt. Der frühere Bundesinnenminister Otto Schily hatte per Dienstanweisung dem Bundesamt für Verfassungsschutz und dem Bundesnachrichtendienst dieses Ermittlungsinstrument genehmigt.

Der Bundesgerichtshof hatte jedoch bereits am 31.01.2007 die Online–Durchsuchungen für Zwecke der Strafverfolgung mangels Rechtsgrundlage für rechtswidrig erklärt.[42] Daraufhin musste auch das Bundesinnenministerium seine Aktivitäten einstellen.

Der erste Versuch, eine rechtliche Grundlage zur Durchführung von Online-Durchsuchungen zu schaffen, war eine Änderung des Verfassungsschutzgesetzes in Nordrhein–Westfalen im Dezember 2006. Danach sollte der Versfassungsschutzbehörde zur Informationsbeschaffung "[...] heimliches Beobachten und sonstiges Aufklären des Internets, wie insbesondere die verdeckte Teilnahme an seinen Kommunikationseinrichtungen bzw. die Suche nach ihnen, sowie der heimliche Zugriff auf informationstechnische Systeme auch mit Einsatz technischer Mittel [...] " erlaubt sein.[43] Damit war die Online–Durchsuchung zum ersten Mal ausdrücklich gesetzlich verankert. Gegen diese Rechtsnorm des VSG NRW wurde Verfassungsbeschwerde vor dem Bundesverfassungsgericht eingelegt. Das Gericht gab der Beschwerde am 27. Februar 2008 statt und erklärte die Vorschrift für verfassungswidrig und somit für nichtig.[44]

[42] BGH, Beschluss vom 31.01.07, StB 18/06
[43] LandtagNRW, LT-Dr 14/2211, S.4, § 5 Abs. 2 Nr. 11 VSG NRW.
[44] BVerfG, 1 BvR 370/07 vom 27.2.2008.

7.4 Das Computer–Grundrecht

Das Verfassungsgericht hat in seiner Entscheidung die heimliche Infiltration von informationstechnischen Systemen zwar nicht grundsätzlich für unzulässig erklärt, hierfür aber strenge Anforderungen aufgestellt und zudem das neue "Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität[45] informationstechnischer Systeme" entwickelt. [46]

Schutzbereich

Das neue Grundrecht wurde aus dem allgemeinen Persönlichkeitsrecht abgeleitet. Als Begründung haben die entscheidenden Richter angegeben, dass die Nutzung der IT–Systeme für die Persönlichkeitsentfaltung vieler Bürger von zentraler Bedeutung sei, aber auch Gefährdungen der Persönlichkeit mit sich bringe.[47] Die Überwachung und Auswertung der Nutzung solcher Systeme ermöglicht nämlich weitreichende Rückschlüsse auf die Persönlichkeit des Nutzers bis hin zu einer Profilbildung.

Das Computer–Grundrecht ist demnach anzuwenden, wenn ein Eingriff IT–Systeme erfasst, die "[...] personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten. [...]"[48]

[45] Vertraulichkeit bedeutet, dass Informationen nur berechtigten Personen bekannt werden. Integrität bedeutet, dass Informationen vollständig, richtig und aktuell sind oder deutlich zu erkennen ist, dass dies nicht der Fall ist. Vgl. Roggan(Hrsg.), Hansen/ Pfitzmann, Techniken der Online-Durchsuchung: Gebrauch, Missbrauch, Empfehlungen, S. 132

[46] Im Folgenden: IT-Grundrecht oder Computer-Grundrecht

[47] BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz–Nr. 170-171.

[48] BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz–Nr. 203.

Geschützt werden soll das Interesse des Nutzers, dass die von einem System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben. Ein Eingriff in dieses Grundrecht ist zudem dann anzunehmen, wenn die Integrität des geschützten informationstechnischen Systems angetastet wird, indem auf das System so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können.[49]

Die Entwicklung des neuen Grundrechts war erforderlich, da die bestehenden Regelungen des Grundgesetzes die Bürger nicht ausreichend vor Online–Durchsuchungen geschützt haben. Die bisher schon vorhandene Grundrechte auf Telekommunikationsfreiheit, Schutz der Wohnung, Schutz der Privatsphäre und das Recht auf informationelle Selbstbestimmung erfassen nicht alle Aspekte der Computernutzung.

a). Abgrenzung zu Art. 10 GG

Der Schutzbereich des Telekommunikationsgeheimnisses umfasst nach Art. 10 GG die Telekommunikation und deren nähere Umstände. Insofern unterliegt auch die Kommunikation über das Internet, insbesondere der E–Mail–Verkehr und die Form des Telefonierens über das Internet, dem herkömmlichen Schutz des Art. 10 GG.

Der Schutz des Fernmeldegeheimnisses erstreckt sich aber nur auf die laufende Kommunikation und endet in dem Moment, in dem die Nachricht beim Empfänger angekommen und der Übertragungsvorgang beendet ist.

Nicht geschützt bleiben also nach dem Abschluss eines Kommunikationsvorganges die gespeicherten Inhalte und Umstände der Telekommunikation, für die der Teilnehmer eigene Schutzvorkehrungen gegen den heimlichen Datenzugriff treffen kann, wie etwa Passwortschutz. Die Daten unterscheiden sich dann nicht

[49]BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz–Nr. 204.

mehr von Daten, die der Nutzer selbst angelegt hat. Die Gefahren, die mit der Übermittlung verbunden sind, bestehen dann nicht mehr.[50]

Der Schutz des Telekommunikationsgeheimnisses besteht auch dann nicht, wenn die Nutzung des Systems durch eine staatliche Stelle als solche überwacht wird oder die Speichermedien des Systems durchsucht werden, es werden insbesondere auch Daten erfasst, die keinen Bezug zu der Telekommunikation aufweisen.

Diese Schutzlücke soll durch das neue Computer–Grundrecht geschlossen werden.

b). Abgrenzung zu Art. 13 GG

Auch die Garantie der Unverletzlichkeit der Wohnung bietet keinen lückenlosen Schutz bezüglich der Zugriffe auf informationstechnische Systeme.

Schutzgut des Art. 13 GG ist nach Formulierung des Bundesverfassungsgerichts die "räumliche Sphäre, in der sich das Privatleben entfaltet."[51]

Insbesondere besteht der Schutz vor dem physischen Eindringen zum Zwecke der Manipulation von IT–Systemen sowie der Wahrnehmung von Vorgängen in der Wohnung. Dazu zählt z.B. die akustische und optische Wohnraumüberwachung, die Messung der elektromagnetischen Abstrahlung von Computern, die in einer Wohnung benutzt werden oder das Eindringen in eine Wohnung, um die RFS zu installieren.

Art. 13 GG gibt aber keinen generellen, von den Zugriffsmodalitäten unabhängigen Schutz gegen die Installation der Schadsoftware über Netzwerke sowie gegen dadurch ermöglichte spätere Zugriffe, auch wenn sich dieses System in der Wohnung befindet.

[50]BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz–Nr. 185.
[51]BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz–Nr. 192 ff.

Weiterhin erfolgen die Online–Durchsuchungen unabhängig vom Standort des IT–Systems. Für die Durchsuchungen ist nicht einmal erkennbar, ob sich der Rechner innerhalb oder außerhalb der Wohnung befindet. Es fehlt bei diesem Eingriff also an der Raumbezogenheit, so dass hier wieder das Computer–Grundrecht eingreift.

c). Abgrenzung zum Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m Art. 1 Abs. 1 GG)

Dieses im "Volkszählungsurteil" im Jahre 1983 geschaffene Grundrecht gibt dem Einzelnen die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.[52]

Der Schutz beschränkt sich auf diejenigen Daten, die der Privatsphäre des Nutzers eines IT–Systems zuzuordnen sind und bewusst erhoben werden. Aus dem Nutzungsverhalten sowie aus den gespeicherten nicht privaten Daten lässt sich ebenfalls auf persönliche Eigenschaften oder Vorlieben schließen. Hier greift aber das Recht auf informationelle Selbstbestimmung nicht. Das neue Grundrecht soll nun die festgestellten Regelungslücken füllen.

Schranken

Wie alle anderen Grundrechte hat auch das neue Computer–Grundrecht Schranken, insbesondere in Bezug auf die Online–Durchsuchung. Nachfolgend soll dargestellt werden, welche Voraussetzungen erfüllt sein müssen, um den Eingriff durchführen zu können.

a). Erforderlichkeit

In erster Linie muss die Erforderlichkeit einer Online–Durchsuchung geprüft

[52]BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz–Nr. 198 ff.

werden. Die offene Durchsuchung ist als milderes Mittel vorzugswürdig, wenn diese ermittlungstechnisch sinnvoll und möglich ist.

Ein heimlicher Zugriff sollte eher eine Ausnahme bleiben und muss besonders gerechtfertigt werden, denn auf diese Weise kann die Behörde an Informationen gelangen, die weitgehende Rückschlüsse auf die Persönlichkeit des Betroffenen bis hin zum Erstellen von Verhaltens–und Kommunikationsprofilen ermöglichen. In Einzelfällen werden notwendigerweise auch Dritte erfasst, wodurch der Eingriff eine große Streubreite erfährt und mittelbar die Freiheit der Bürger beeinträchtigt.[53]

b). Verhältnismäßigkeit

Es müssen tatsächliche Anhaltspunkte und eine konkrete Gefahr für ein überragend wichtiges Rechtsgut wie Leib, Leben, Freiheit der Person, Bestand des Staates oder Grundlage der Existenz des Menschen vorliegen (z.B. Terroranschläge, Mord, Geiselnahme).

c). Richtervorbehalt

Außerdem gilt für den heimlichen Zugriff auf IT-Systeme ein Vorbehalt richterlicher Anordnung. Da es sich um eine heimliche Maßnahme handelt, versagt der gerichtliche Rechtsschutz, und der Betroffene kann durch sein Verhalten nicht auf den Gang der Ermittlungen einwirken. Dies soll durch die vorbeugende Kontrolle einer unabhängigen Instanz kompensiert werden.[54]

d). Kernbereichsschutz

Der Kernbereich privater Lebensgestaltung muss durch den Staat gewahrt werden, indem ein Eingriff auch nicht durch überwiegendes Interesse der Allge-

[53]BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz–Nr. 232-233.
[54]BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz–Nr. 258.

meinheit zu rechtfertigen ist. Es betrifft z.B. solche Daten, wie tagebuchartige Aufzeichnungen oder private Film– und Tondokumente.[55]

Das BVerfG hat diesbezüglich ein zweistufiges Konzept entwickelt. Bei der Erhebung der Daten muss soweit wie möglich sicherstellt werden, dass keine Daten mit Kernbereichsbezug erhoben werden. In der Auswertungsphase sind dann die dennoch erhobenen Kernbereichsdaten unverzüglich zu löschen und ihre Verwertung und Weitergabe auszuschließen.[56]

7.5 Gesetzliche Einführung der Online–Durchsuchung

Gemäß § 31 BVerfGG binden die Entscheidungen des Bundesverfassungsgerichts die Verfassungsorgane des Bundes und der Länder sowie alle Gerichte und Behörden.

a). Bundesebene: BKAG
Die strengen Anforderungen aus dem Urteil des BVerfG wurden nun in einem "Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt" umgesetzt. Das geänderte BKA–Gesetz ist am 1. Januar 2009 in Kraft getreten.[57]

Danach darf das BKA zur Abwehr terroristischer Gefahren Online–Durchsuchungen von Computern und anderen IT–Systemen durchführen. Das wird in § 20k BKAG mit der amtlichen Überschrift "Verdeckter Eingriff in informationstechnische Systeme" geregelt.

Es wird eine "Remote Forensic Software" für die Durchführung der Online–Durchsuchung eingesetzt. Die Beamten dürfen zur Installation der Software

[55] BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz–Nr. 270 ff.
[56] BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz–Nr. 280 ff.
[57] Bundeskriminalamtgesetz vom 7. Juli 1997 (BGBl. I S. 1650), das zuletzt durch Art. 1 des Gesetzes vom 6. Juni 2009 (BGbl. I S. 1226) geändert worden ist.

aber nicht in die Wohnungen von Verdächtigen eindringen, sodass in der Regel nur der Weg über das Internet offen steht.

Die Überwachung darf nur für einen Zeitraum von bis zu drei Monaten erfolgen, wobei jeweils eine Fristverlängerung von maximal drei Monaten möglich ist, soweit die Gefahren und Voraussetzungen für die Maßnahme unter Berücksichtigung der gewonnenen Kenntnisse weiterhin vorliegen.

Gegen das BKA–Gesetz wurde allerdings bereits im Januar 2009 wiederum eine Verfassungsbeschwerde beim BVerfG eingereicht. Diese richtet sich insbesondere gegen die Befugnisse des BKA zur Online–Durchsuchung und Telekommunikationsüberwachung.

b). Länderebene: Bayern
Auf der Länderebene dürfen zumindest in Bayern die Polizei und das Landesamt für Verfassungsschutz ab dem 1. August 2008 heimliche Online–Durchsuchungen durchführen.

7.6 Beweissicherheit

Wenn man elektronisch gespeicherte Daten auf IT–Systemen als rechtskräftige Beweise vor Gericht verwenden will, sind eine Reihe technisch–organisatorischer Anforderungen umzusetzen. Es muss nicht nur ein rechtsstaatlich korrektes Vorgehen der Ermittler garantiert werden, sondern auch sichergestellt werden, dass die erhobenen Daten tatsächlich von der verdächtigen Person stammen und von niemandem manipuliert worden sind.[58]

[58]Hansen/Pfitzmann Windei Bundestrojaner. Online–Durchsuchung vs. Gewährleistung von Vertraulichkeit und Integrität informationstechnischer Systeme, S. 89.

Computer–Forensik

So setzt die konventionelle Computer–Forensik auf garantierte Unveränderlichkeit des Untersuchungsgegenstandes. Um Veränderungen auszuschließen, werden sichergestellte Festplatten schreibgeschützt ausgelesen und eine Image–Kopie erstellt. Anschließend werden anhand der Image–Kopie inhaltliche Untersuchungen vorgenommen und dokumentiert.[59]

Die herkömmlichen Durchsuchungen und Beschlagnahmen helfen aber nicht weiter, wenn die Daten z.B. bereits gelöscht (nicht nur oberflächlich), mit einem Passwort geschützt oder verschlüsselt worden sind. In diesen Fällen kommen die Ermittler an die Daten nicht mehr heran. Probleme bereiten auch die Datenträger, die schnell zerstörbar bzw. löschbar oder leicht zu verstecken sind, wie z.B. das Smartphone mit Sofortlöschungsfunktion oder USB–Sticks.

Mittels der Online–Durchsuchung wollen die Ermittler Klardaten oder zumindest die verwendeten Passwörter und Krypto–Keys sicherstellen.

Beweiskraft der Online–Durchsuchungen

Im Gegensatz zur forensischen Analyse ist bei einer Online–Durchsuchung die Veränderung des Untersuchungsgegenstandes eine Voraussetzung für die Durchführung der Maßnahme, bedingt durch das Einbringen einer RFS auf das Zielsystem. Dazu kommt, dass das IT–System während der Datenerhebung weiterhin genutzt wird, so dass weitere Veränderungen nicht ausgeschlossen sind.

Es kann auch nicht garantiert werden, dass die gewonnenen Informationen tatsächlich nur von der verdächtigen Person stammen. Bei der Online–Durchsuchung wird nur das IT–System identifiziert und nicht die Person, die das System

[59] Hansen/Pfitzmann Technische Grundlagen von Online–Durchsuchung und –Beschlagnahme. Artikel für Deutsche Richterzeitung, S. 225–228.

benutzt. Es ist möglich, dass das IT–System von mehreren Personen gleichzeitig genutzt wird. Der Zugriff Dritter ist ebenfalls nicht ausgeschlossen. Dabei können Fehler in der RFS ausgenutzt werden oder auch andere Schadsoftware benutzt werden.

Auch die angeblich lückenlose Protokollierung aller Aktivitäten und die Hinterlegung des Quellcodes der RFS bei Gericht[60] kann nicht garantieren, dass Daten auf dem Zielsystem nicht verändert werden. Weiterhin ist nicht auszuschließen, dass die RFS entdeckt werden und die Daten bei der Übertragung zu den Ermittlern absichtlich manipuliert werden.

Demzufolge ist der Beweiswert der gewonnenen Daten stark zu bezweifeln.

7.7 Weitere Kritikpunkte

Reichweite der Eingriffe

Die Reichweite der Eingriffe ist kaum einzuschätzen. Bereits bei den Online–Durchsuchungen von Einzelsystemen ist davon auszugehen, dass nicht nur Einzelpersonen überwacht werden. Wenn beispielsweise mehrere Personen das Zielsystem nutzen, sind sie alle von der Maßnahme betroffen.

Bei dem Begriff IT–System ist aber auch nicht auszuschließen, dass Server und Netzwerke überwacht werden. Die Anzahl der Betroffenen ist dann dementsprechend hoch.[61] Es ist zu bedenken, dass auch versehentlich das falsche System überwacht werden könnte, da die dynamisch mit dem Internet verbundenen Rechner sich in der Regel nicht hinreichend eindeutig adressieren lassen. Auf diese Weise werden völlig Unbeteiligte durch den Eingriff geschädigt.

[60] BMI Fragenkatalog der SPD-Bundestagsfraktion, AG Kultur und Medien, AG Neue Medien, S. 4, 14.

[61] Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, S. 8.

IT–Sicherheit

Ein weiterer Kritikpunkt ist die IT–Sicherheit des Zielrechners. Auch eine staatliche Durchsuchungssoftware kann Fehler enthalten. Es ist deswegen fraglich, ob die RFS unentdeckt bleiben oder der Missbrauch durch Dritte ausgeschlossen werden kann.

Schutz des Kernbereichs privater Lebensgestaltung

Kritisiert wird zudem, dass der Kernbereich privater Lebensgestaltung bei einer Online–Durchsuchung nicht ausreichend geschützt wird. Es gibt kein geeignetes technisches Verfahren, dass die Erhebung der Daten aus dem Kernbereich vollständig ausschließen lässt. Beispielsweise kann nicht garantiert werden, dass bestimmte Dateinamen oder Dateiendungen von der Maßnahme unberührt bleiben. Auch ein Filtern nach Schlüsselwörtern ist nicht zielführend, sodass im Endeffekt der gesamte Datenbestand der Zielperson übertragen und duchgesehen werden müsste. Dies stellt einen massiven Eingriff in den Kernbereich der Privatsphäre des Betroffenen dar.

Wenig Erfolg versprechend

Es wird auch stark bezweifelt, dass die Zielsetzung der Bekämpfung von Terrorismus oder organisierter Kriminalität mit Online–Durchsuchungen erreicht werden kann, da gerade diese Personengruppen sich gegen die Zugriffe auf einfache Weise schützen können.

Man kann bspw. vertrauliche Informationen auf einem vom Internet getrenntem IT–System erstellen und dort verschlüsseln, dann auf anderes System überspielen, so dass dieses System nur die verschlüsselten Daten enthält. Zur Übertragung der Informationen per Internet kann dann immer ein anderer In-

ternet–Anschluss genutzt werden, sodass die Lokalisierung des Systems, in dem die Daten in unverschlüsselter Form vorliegen nahezu unmöglich ist.[62]

Der "Bundestrojaner" kann daher nur bei technisch unbegabten Terroristen funktionieren, bei den wohl auch herkömmliche Ermittlungsmethoden ausreichend wären, sodass die Verhälnissmäßigkeit bei der Online–Durchsuchung nicht gegeben ist.

Zusätzlich gerät der Staat in einen Zielkonflikt, da einerseits das Bundesamt für Sicherheit in der Informationstechnik die IT–Sicherheit fördern will, aber andererseits diese durch die Maßnahmen zur Online–Durchsuchung verhindert würde.

[62]Hansen/Pfitzmann Windei Bundestrojaner. Online–Durchsuchung vs. Gewährleistung von Vertraulichkeit und Integrität informationstechnischer Systeme, S. 91.

8 Zusammenfassung

In dieser Arbeit wurden verschiedene Möglichkeiten staatlicher Überwachung der individuellen Kommunikation aufgezeigt. Angefangen wurde mit der Beschreibung der Telekommunikationsüberwachung und der Vorratsdatenspeicherung. Im Anschluss daran fand die Behandlung der Online–Durchsuchung mit Hilfe des Bundestrojaners statt. Dies sind wirkungsvolle Werkzeuge um in die Privatsphäre der Staatsbürger einzudringen. Aber der Verwendung dieser Maßnahmen sind enge Grenzen gesetzt. Die wichtigsten Grundrechte auf die sich die Bürger berufen können ist das Computergrundrecht und der Artikel 10 GG. Um diese Fundamentalrechte zu beschränken, sind Eingriffsnormen notwendig, welche in den vorangegangenen Kapiteln vorgestellt wurden. Die rechtmäßige Anwendung dieser juristischen Normen kann von der Judikative überprüft werden. Somit ist der mündige Staatsbürger den überwachenden, staatlichen Organen nicht hilflos ausgeliefert, sondern kann sich juristisch zur Wehr setzen.

A Abkürzungsverzeichnis

Art.	Artikel
BGH	Bundesgerichtshof
BMI	Bundesministerium des Inneren
BMJ	Bundesministerium der Justiz
BKA	Bundeskriminalamt
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVerfG	Bundesverfassungsgericht
BVerfGG	Bundesverfassungsgerichtsgesetz
EG	Europäische Gemeinschaft
G10	Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses
GG	Grundgesetz
Hrsg.	Herausgeber
IT-System	Informationstechnisches System
Quellen-TKÜ	Quellen–Telekommunikationsüberwachung
RFS	Remote Forensic Software
SMS	Short Message Service

StPo	Strafprozessordnung
TKG	Telekommunikationsgesetz
VSG NRW	Verfassungsschutzgesetz Nordrhein-Westfalen

B Aufteilung

Swetlana Klaus

Kapitel 7 - Online Durchsuchung / Computergrundrecht

Andreas Grüner

Kapitel 1 - Einleitung, Kapitel 2 - Grundrechte, Kapitel 3 - Datenarten, Kapitel 4 - Artikel 10 Grundgesetz, Kapitel 5 - Telekommunikationsüberwachung, Kapitel 6 - Vorratsdatenspeicherung, Kapitel 8 - Zusammenfassung

Literatur

2006/24/EG: 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.

Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Technische Aspekte der Online–Durchsuchung. 21.09.2007. ⟨Internet: `http://www.lfd.m-v.de/dschutz/informat/internet/onlinedurchsuchung.pdf[30.09.2009]`⟩

BGBl. I: Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt. Bundesgesetzblatt Jahrgang 2008 Teil I Nr. 66. 31.12.2008. ⟨Internet: `http://www.bgblportal.de/BGBL/bgbl1f/bgbl108s3083.pdf[30.09.2009]`⟩, 3083–3094

BMI: Fragenkatalog der SPD-Bundestagsfraktion, AG Kultur und Medien, AG Neue Medien. 22.08.2007. ⟨Internet: `http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf[30.09.2009]`⟩

BMI: Fragenkatalog des Bundesministeriums der Justiz. 22.08.2007. ⟨Internet: `http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf[30.09.2009]`⟩

Bultmann, Peter Friedrich: Öffentliches Recht mit Vertiefung im Gewerbe-,

Wettbewerbs-, Subventions- und Vergaberecht. Berlin Heidelberg: Springer Verlag. 2008.

BVerfG: Leitsätze zum Urteil des Ersten Senats vom 27. Februar 2008. Zitierung: BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. (1 - 333). 27.02.2008. ⟨Internet: `http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html[30.09.2009]`⟩

BVerfSchG: Bundesverfassungsschutzgesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2970), das zuletzt durch Artikel 1a des Gesetzes vom 31. Juli 2009 (BGBl. I S. 2499) geändert worden ist.

Cremer, Wolfgang: Freiheitsgrundrechte. Funktionen und Strukturen. Tübingen: Mohr Siebeck. 2004.

Duden: Recht A-Z. Fachlexikon für Studium, Ausbildung und Beruf. ⟨Internet: `http://www1.bpb.de/wissen/ZDS2GS,0,0,Wesensgehaltsgarantie.html[26.09.2009]`⟩

EGV: EG-Vertrag (Vertrag zur Gründung der Europäischen Gemeinschaft). In der Fassung vom 02.10.1997. Zuletzt geändert durch den Vertrag über den Beitritt der Republik Bulgarien und Rumäniens zur Europäischen Union vom 25.4.2005 (ABl. EG Nr. L 157/11) m.W.v. 1.1.2007.

Eike Albrecht, Benjamin Küchenhoff: Staatsrecht. Lehrbuch. Berlin: Erich Schmidt Verlag. 2008.

Fox, Dirk: Stellungnahme zur „Online-Durchsuchung“. Verfassungsbeschwerden 1 BvR 370/07 und 1 BvR 595/07. 29.09.2007. ⟨Internet: `http://www.secorvo.de/publikationen/`

stellungnahme-secorvo-bverfg-online-durchsuchung.pdf[30.09.2009]⟩

G10: Artikel 10-Gesetz vom 26. Juni 2001 (BGBl. I S. 1254, 2298), das zuletzt durch Artikel 1 des Gesetzes vom 31. Juli 2009 (BGBl. I S. 2499) geändert worden ist.

Gailus, Andrea: Das BKA-Gesetz. Weitreichende Befugnisse. 29.04.2009. ⟨Internet: http://www.datenschutz-praxis.de/fachwissen/fachartikel/das-bka-gesetz[30.09.2009]⟩

Groepl, Christoph: Brief-, Post- und Fernmeldegeheimnis, Art. 10 GG. ⟨Internet: http://www.groepl.uni-saarland.de/lehre/lehre09/GR17.pdf[26.09.2009]⟩

Hansen, Markus/Pfitzmann, Andreas: Windei Bundestrojaner. Online–Durchsuchung vs. Gewährleistung von Vertraulichkeit und Integrität informationstechnischer Systeme. c't/25. 2008. ⟨Internet: http://www.heise.de/ct/Online-Durchsuchung--/artikel/126529[30.09.2009]⟩

Hansen, Markus/Pfitzmann, Andreas: Technische Grundlagen von Online–Durchsuchung und –Beschlagnahme. Artikel für Deutsche Richterzeitung, S. 225–228. August 2007. ⟨Internet: https://tepin.aiki.de/blog/uploads/hansen-pfitzmann-online-durchsuchung-und-beschlagnahme-1.0.pdf[30.09.2009]⟩

Hesselberger, Dieter: Das Grundgesetz. Kommentar für die politische Bildung. Wolters Kluwer Deutschland GmbH. 2003.

Holzner, Stefan: Die Online–Durchsuchung: Entwicklung eines neuen Grundrechts. Kenzingen: Centaurus Verlag. 2009.

Katz, Alfred: Staatsrecht. Grundkurs im öffentlichen Recht. Heidelberg: C. F. Müller Verlag. 2002.

Keller, Christoph: Telekommunikationsüberwachung und andere verdeckte Ermittlungsmaßnahmen. Stuttgart: Richard Boorberg Verlag. 2008.

LandtagNRW: Gesetzesentwurf der Landesregierung NRW, 14. Wahlperiode LT-Dr. 14/2211. 03.07.2006. ⟨Internet: `http://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMD14-2211.pdf[30.09.2009]`⟩

LG Köln: Urteil vom 06.09.2006. Az. 280178/06.

Roggan, Fredrik (Hrsg.): Online-Durchsuchungen. Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar 2008. Berlin: BWV Berliner Wissenschaft-Verlag. 2008.

StGB: Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), das zuletzt durch Artikel 3 des Gesetzes vom 2. Oktober 2009 (BGBl. I S. 3214) geändert worden ist.

StPO: Strafprozeßordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 3 des Gesetzes vom 30. Juli 2009 (BGBl. I S. 2437) geändert worden ist.

TKG: Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch Artikel 2 des Gesetzes vom 14. August 2009 (BGBl. I S. 2821) geändert worden ist.

TKGuaÄndG: Artikel 2 des Gesetzes vom 14. August 2009 (BGBl. I S. 2821).

Vorratsdatenspeicherung: Sammel-Verfassungsbeschwerde gegen Vorratsdatenspeicherung. ⟨Internet: `http://www.vorratsdatenspeicherung.de/content/view/51/70/lang,de/[26.09.2009]`⟩