



Lothar Binding
Mitglied des Deutschen Bundestages

Innere Sicherheit kostet uns Persönlichkeitsrechte und Datenschutz – aber alles hat seinen Preis?

Am 4. September 2007 wurden drei Verdächtige festgenommen. Die drei Männer - zwei zum Islam konvertierte Deutsche und ein Türke - hatten nach Erkenntnissen der Ermittler Bombenanschläge auf US-amerikanische Einrichtungen geplant und konnten nach monatelangen Ermittlungen festgenommen werden. Bei den Anschlagplanungen nutzten die Verdächtigen mehr als 100 Callcenter und Internetcafes und 17 verschiedene Laptops.

Die einfache, teils zu einfache Forderung von einigen Ermittlungsbehörden und Innenpolitikern lautete: Für eine wirksame Verfolgung und Bekämpfung von Straftaten sei der verdeckte Zugriff auf Telekommunikationsdaten und Computerfestplatten Verdächtiger erforderlich, argumentieren die Befürworter der Vorratsdatenspeicherung und der Online-Durchsuchung. Deshalb müsse man diese Daten über einen gewissen Zeitraum einsehen und speichern dürfen. Potentielle Gefahren rechtzeitig zu erkennen und verdächtige Personen aus dem Verkehr zu ziehen – so lautet das Ziel für jene Politiker und Behörden, die Verantwortung für unsere Innere Sicherheit übernehmen.

Mit dem Instrument der heimlichen Online- Durchsuchung soll mittels eines eingeschleusten Virusprogramms Daten des PC- Inhabers auf einen Polizeicomputer gespeichert werden, um sie nach belastenden Informationen durchforsten zu können - ohne das Wissen des Betroffenen. Ermittlungsbehörden erhoffen sich von diesem Zugriff auf Computerfestplatten Erleichterungen bei der Verbrechensbekämpfung. Gleiches gilt für die sog. Verkehrs- und Standortdaten bei der Telekommunikation. Dabei handelt es sich um Daten, die entstehen, wenn man telefoniert, ein Fax sendet, im Internet surft, sich mit anderen in einem *Chatroom* unterhält oder eine E- Mail verschickt. Sie enthalten Informationen über IP- Adressen, Datum, Uhrzeit und Dauer der Verbindung sowie die dabei übertragene Datenmenge.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder betonte hingegen in einer Pressemitteilung vom März 2007, dass die Vorratsdatenspeicherung in Widerspruch zur Verfassung und zur Rechtsprechung des Bundesverfassungsgerichtes stehe. Zudem beeinträchtige sie „die für eine freiheitliche Gesellschaft konstitutive unbefangene Kommunikation erheblich“.

Die Frage nach der Erlaubnis zur Vorratsdatenspeicherung und zur Onlinedurchsuchung berührt wichtige Aspekte unseres Staatsverständnisses. Eine der fundamentalen Aufgaben unseres demokratischen Gemeinwesens ist der grundgesetzlich verankerte Schutz der Menschen- und Bürgerrechte. Sie sind ihrem Wesen und Ursprung nach Abwehrrechte gegenüber staatlicher Willkür, bilden die Richtschnur für das gesamte staatliche Handeln und setzen ihm klare Grenzen. In der SPD arbeiten wir für einen solchen demokratischen

Rechtsstaat, der staatliche Macht begrenzt und die sozialdemokratischen Grundwerte Freiheit, Gerechtigkeit und Solidarität gewährleistet.

Gleichzeitig setzt sich der Rechtsstaat aber auch die Aufgabe, seine Bürgerinnen und Bürger zu schützen, ihr Hab und Gut zu verteidigen und sie vor Angriffen auf ihr leibliches Wohl zu bewahren. Dieses Sicherheitsinteresse ist eine der zentralen Herausforderungen des modernen Staates. Zu diesem Zweck verfügt er bereits über wirksame Instrumente der Strafverfolgung und der Gefahrenabwehr, die die Grenzen, die das Grundgesetz setzt, respektieren.

Beide Aufgaben – Schutz der bürgerlichen Freiheiten und Verantwortung für die innere und äußere Sicherheit - haben ihre normative Berechtigung. Zum Dilemma werden sie allerdings in einer Entscheidungssituation, in der die Verfolgung eines Ziels nur auf Kosten des anderen gelingen kann.

Die Gruppe für den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, die sog. Artikel 29- Datenschutzgruppe der Europäischen Union, hat eine treffende Formulierung für dieses Dilemma gefunden:

„Die Aufbewahrung von Verkehrsdaten ist ein Eingriff in das unverletzliche Grundrecht auf Achtung des Brief-, Post- und Fernmeldegeheimnisses. Eingriffe in dieses Grundrecht müssen einem zwingenden Bedarf entspringen, sie sollten nur in Ausnahmefällen gestattet werden und angemessenen Schutzmaßnahmen unterworfen sein. Der Terrorismus stellt unsere Gesellschaft vor eine reale und drängende Herausforderung. Die Regierungen müssen auf diese Herausforderung in einer Form reagieren, die dem Bedürfnis der Bürger, in Frieden und Sicherheit zu leben, wirkungsvoll nachkommt, ohne die Menschenrechte des Einzelnen, darunter das Recht auf Privatsphäre und Datenschutz, auszuhöhlen, denn diese Rechte gehören zu den Eckpfeilern unserer demokratischen Gesellschaft.“ (Artikel 29- Datenschutzgruppe, 1868/05/DE)

Ein Staat, der nicht in der Lage ist, seine Bürger vor terroristischen Angriffen und kriminellen Machenschaften zu schützen, hat schwerwiegende Defizite aufzuweisen. Wo der Schutz der Bürger jedoch nur durch die Außerkraftsetzung der Menschen- und Bürgerrechte gelingt, stehen wir vor ernsthaften Legitimationsproblemen.

Die Balance zwischen diesen beiden Zielvorgaben zu finden, ist schwierig. Nicht immer komme ich bei politischen Entscheidungen zu einer Position, die für beide Seiten eine *win-win*- Situation darstellt und meine volle Zustimmung hat. Gelegentlich muss ich zwischen Zielen abwägen, die in einem Spannungsverhältnis zueinander stehen – und bisweilen lassen sich für juristisch komplexe und politisch sensible Probleme keine einfachen Lösungen finden, die alle Seiten zufriedenstellen.

Seit der Föderalismusreform ist der Bund für die polizeiliche Gefahrenabwehr zuständig, das BKA verfügt über die Präventionsbefugnis. Der rasante Übergang ins Informationszeitalter bietet Ermittlungsbehörden neue Möglichkeiten, Gesetzesverstöße aufzuspüren, zu verfolgen und zu ahnden. Technische Weiterentwicklungen, die Daten, Protokolle und Profile speichern, erlauben auch eine Weiterentwicklung der Überwachungsinfrastruktur und einen immer tieferen Zugriff auf persönliche Daten. Wenn sich die Informations- und Kommunikationstechnik weiterentwickelt und lediglich abstrakte Eingriffsbefugnisse definiert werden, müssen wir auf Ausgewogenheit und Verhältnismäßigkeit der Mittel achten.

Denn nicht alles, was technisch machbar ist, ist auch politisch sinnvoll und rechtlich zulässig. Wo Daten, die den Kernbereich der privaten Lebensgestaltung betreffen, gespeichert werden bzw. dem Zugriff der Ermittler offenstehen sollen, stößt das Strafverfolgungsinteresse des Staates in einen sensiblen Bereich vor. Diese Daten müssen durch ein absolutes Verwertungsverbot geschützt werden. Dies gilt besonders dann, wenn die Einleitung strafrechtlicher Ermittlungsverfahren nicht mehr von einem konkreten Tatverdacht abhängig sein soll. Denn die Grundrechte und politischen Prinzipien des Rechtsstaates sind keine Variablen, die je nach Sicherheitslage und Bedrohungsszenario neu festgelegt werden können.

Diese unbedingte Schranke für Ermittlungsbehörden hat das Bundesverfassungsgericht definiert und gestärkt. Im Jahr 2005 etwa hat das Bundesverfassungsgericht das Umsetzungsgesetz zum EU- Haftbefehl und die Telefonüberwachung nach niedersächsischem Landesrecht für unvereinbar mit dem Grundgesetz erklärt. Gleiches galt für die Rasterfahndung oder das Luftsicherheitsgesetz. Auch die SPD- Bundestagsfraktion verteidigt diese Linie und hat die geplante Vorratsdatenspeicherung von Fingerabdrücken, die zur Erstellung biometrischer Pässe genommen wurden, abgelehnt.

ONLINE- DURCHSUCHUNG (REMOTE FORENSIC SOFTWARE)

Rechtliche Aspekte:

Bei der gegenwärtig debattierten Online- Durchsuchung lässt sich das Spannungsverhältnis zwischen Sicherheitsbedürfnis und Grundrechtsschutz exemplarisch nachzeichnen. Denn das staatliche „Ausspähen“ von Festplatten ist ein virtuelles Eindringen in den grundrechtlich geschützten Bereich der Wohnung und der Privatsphäre. Viele Computernutzer speichern auch persönliche Informationen auf ihren Festplatten, bspw. Kontodaten, Bilder, Krankenunterlagen, Tagebücher etc. Das Bundesverfassungsgericht nennt in seiner Rechtsprechung diesen Bereich „das letzte Refugium zur Wahrung der Menschenwürde“. Der Bundesgerichtshof ist dieser Maxime des Bundesverfassungsgerichtes gefolgt und hat die Praxis der Online- Durchsuchung verboten, da keine ausreichende gesetzliche Grundlage vorhanden war.

Angesichts neuer technischer Herausforderungen und Möglichkeiten stellt sich allerdings auch das Problem, wie man Grundrechtsschutz adäquat definieren kann, bspw. entlang folgender Fragen:

- Ist der Grundsatz der Achtung der Unverletzlichkeit der Wohnung (Art. 13 GG) außer Kraft gesetzt angesichts mobil einsetzbarer Hardware wie Laptops, Mobiltelefone, Handhelds ...?
- Stellt der verdeckte Zugriff auf Daten, die auf einer Festplatte gespeichert und nicht Gegenstand der Kommunikation des Computernutzers mit anderen sind (bspw. Kontodaten, Notizen, technische Skizzen ...) eine Einschränkung des Schutz des Fernmelde- und Postgeheimnisses (Art. 10 GG) dar?
- Stellt die Speicherung von Telekommunikationsdaten eine Einschränkung des Grundrechts auf informationelle Selbstbestimmung, d.h. der Offenbarung und Verwendung personenbezogener Daten, dar?
- Wie lässt sich der als besonders schützenswert eingestufte Kernbereich der privaten Lebensführung bei Online- Durchsuchungen technisch abgrenzen?

Was ist technisch machbar und sinnvoll?

Bislang gilt bei der Beweiserhebung in Computersystem folgendes Verfahren, das die Echtheit der gefundenen Dateien belegen und ihre Eignung als Beweismittel nachweisen soll:

- Festplatte wird sichergestellt; damit kann lediglich ein bestimmter Endzustand des Datenträgers analysiert werden
- es wird eine Kopie in Form eines identischen Bildes angefertigt (Image);
- anhand der Kopie - niemals beim Original! - werden inhaltliche Untersuchungen angestellt; denn: „Die Nichtveränderung der sichergestellten Originaldatenträger ist wesentliche Grundlage für die Revisionsfähigkeit und damit die Verlässlichkeit der Untersuchungsmethode.“ (DRiZ 2007/ 225)

Grundproblem bei der technischen Umsetzung der Online- Durchsuchung ist die Gewährleistung eines einheitlichen und nachvollziehbaren Vorgehens der Ermittler über die verschiedenen Phasen, d.h. bei Infiltration, Datengewinnung und Datenübermittlung des Verfahrens hinweg. Es bereitet Schwierigkeiten, die Revisionsfähigkeit auf dem infiltrierten System ist zu gewährleisten, denn schon die Infiltration eines „Bundestrojaners“ stellt eine Veränderung des Zielobjektes dar; zudem besteht die Möglichkeit, dass auch andere Hacker Zugriff auf die Festplatte haben oder bekommen oder der Computernutzer den Angriff bemerkt und bewusst seine eigenen Daten manipuliert. Die Verlässlichkeit der ermittelten Daten ist also nicht zweifelsfrei zu gewährleisten.

Zentrale Aspekte der Debatte um die Online- Durchsuchung

- **Installation der Software:** Die Einbringung kann über eine Internetverbindung - mittels Ausnutzung einer Sicherheitslücke oder durch den Austausch einer Download- Datei - oder durch Installation von einem Datenträger (USB- Stick, CD) erfolgen. Computer-Trojaner tarnen sich meist als harmlose Software: Bildschirmschoner, Videodateien, Zugangsprogramme, Email- Anhänge. Mit der Ausführung eines Programms wird eine verborgene Schadfunktion, meist in Form der Öffnung einer sog. Backdoor, in Gang gesetzt. Dadurch können über die Internetverbindung weitere Schadprogramme auf den infizierten Rechner geladen werden. Trojaner können über verdeckte Kanäle Handlungsanweisungen empfangen, Informationen senden, auf dem System Daten gewinnen und manipulieren.
- **Umfang der Überwachung:** Laut BKA- Chef Ziercke können max. 10 Maßnahmen pro Jahr durchgeführt werden, da die Software jeweils eigens entwickelt werden müsse, um Sicherheitslücken im Betriebssystem und in der Software, die auf dem Zielrechner installiert ist, ausnutzen zu können.

Gegenargument: Die Software- Entwicklung ist weit weniger aufwändig, da sie automatisiert werden kann und nur noch Details in ein Toolkit eingegeben werden müssen. Außerdem arbeiten viele Nutzer und Unternehmen mit Standardkonfigurationen von Software und Betriebssystemen.

- **Datengewinnung:** Ein Bundestrojaner würde umfangreiche Methoden der Datengewinnung ermöglichen. Damit kann eine kontinuierliche Überwachung eines infiltrierten Rechners (Monitoring) durchgeführt werden:
 - Zugriff auf Daten vor der Verschlüsselung (Keystroke- Logger: Programme, die Tastaturbewegungen und Mausbewegungen protokollieren und digitale Bildschirmfotos erstellen und versenden können. Sie umgehen Verschlüsselungsverfahren, da sie Daten wie Passwörter, PINs etc. schon vor deren Verschlüsselung aufzeichnen)
 - Zugriff auf den temporären Arbeitsspeicher und Mitschnitt nur temporär angelegter Dateien möglich, bspw. des Cache- Speichers.
 - Über eine längere Beobachtung des Cache- Speichers lässt sich das Internetnutzungsverhalten des Nutzers rekonstruieren. Im Fall der verschlüsselten Kommunikation ist die Kontrolle des Inhalts überhaupt nur auf diesem Weg möglich.
 - Ebenso können Ermittlungsbehörden durch eine fortlaufende Überwachung auch später gelöschte Daten kopieren und auswerten, auf die Kommunikation mit anderen Rechnern oder auch auf Mikrophone oder Kameras zugreifen, die eine Überwachung der Computerumgebung erlauben.
 - Fernsteuerung des Rechners

- **Grenzen der Telekommunikationsüberwachung:** Das Risiko einer Entdeckung des Bundestrojaners wird als hoch eingeschätzt, da Virenschutzprogramme nicht mehr nur nach bekannten Dateimustern von Schadprogrammen, sog. Signaturen, suchen, sondern auch nach verdächtigen Verhaltensweisen, das sog. heuristische Verfahren. Dadurch entsteht das Problem einer Manipulation eines entdeckten Trojaners.
 - Verschiedene Anwendungen, bspw. Online- Banking, nutzen zudem verschlüsselte Übertragungskanäle: https statt http für WWW- Seiten, POP3S für den Mailabruf, SSL statt SMTP für den Mailversand, SFTP oder SCP statt FTP für den Dateitransfer.
 - Übertragene Daten können nicht zwangsläufig auf ihre Echtheit hin überprüft werden, da keine eindeutig identifizierbare digitale Signatur erkenn- und zuweisbar ist. Beendigung der Maßnahme muss jederzeit möglich sein.
 - Durch den Einsatz von Verschlüsselungssoftware kann der Zugriff auf Festplatten bspw. durch Einrichtung „virtueller Laufwerke“ gänzlich verhindert werden.
 - Auch durch einen Wechsel des Betriebssystems, das von einem schreibgeschützten Datenträger gestartet werden kann (bspw. Linux, MacOS; hier arbeiten Nutzer nur mit eingeschränkten Administratorrechten) lassen sich Infiltrationsversuche leicht abblocken.
 - Auch durch die Abhängigkeit von der Internetverbindung stößt die Online- Durchsuchung an Grenzen: Sie funktioniert zum einen nur bei bestehender Internetverbindung; zum anderen würde eine komplette Spiegelung oder Monitoring aufgrund der begrenzten Kapazitäten in Senderichtung (1024 kBit) sehr viel Zeit in Anspruch nehmen

TELEKOMMUNIKATIONSÜBERWACHUNG UND VORRATSDATENSPEICHERUNG

In dieser Woche stand in 2. und 3. Lesung das Gesetz zur Neuregelung der geltenden Vorschriften der StPO zur Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG zur sog. Vorratsdatenspeicherung auf der Tagesordnung.

Das Gesetz regelt die strafprozessualen heimlichen Ermittlungsmaßnahmen neu und muss am 1. Januar 2008 in Kraft treten, da die geltenden Regelungen über die Abfrage von Telekommunikationsdaten durch Strafverfolgungsbehörden bis Ende diesen Jahres befristet sind. Mit dem Gesetz wird zudem die Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates in nationales Recht umgesetzt, die am 3. Mai 2006 in Kraft getreten ist. Sie muss für Verkehrsdaten aus den Bereichen der Festnetz- und Mobilfunktelephonie noch in diesem Jahr in nationales Recht umgesetzt sein, für Verkehrsdaten aus dem Internetbereich ist ein Aufschub bis 15. März 2009 zulässig. Für den Fall, dass das Umsetzungsgesetz nicht rechtzeitig in Kraft treten könnte, wäre mit einem kostspieligen Vertragsverletzungsverfahren zu rechnen gewesen.

Bei der Einführung der so genannten Vorratsdatenspeicherung geht es im Kern um die künftige Pflicht der Telekommunikationsunternehmen, Daten zu speichern. Wir haben uns gemeinsam mit unserem Koalitionspartner dafür eingesetzt, dass bei der Umsetzung der Richtlinie in nationales Recht keine Regelungen zu Speicherdauer und erfassten Datenarten getroffen werden, die über die Mindestanforderungen der Richtlinie hinausgehen. Diese Selbstbindung hatten wir auch im Koalitionsvertrag festgeschrieben, um die grundlegenden Prinzipien des Datenschutzes - Sparsamkeit und enge Zweckbindung – zu verteidigen.

Die wesentlichen Eckpunkte des TÜ- Gesetzes sind:

- Es ist eine **Mindestspeicherfrist** von 6 Monaten vorgesehen, eine Verlängerung der Frist auf bis zu 24 Monate liegt im Ermessen der einzelnen Mitgliedstaaten. Der Bundestag hat bekräftigt, dass nicht über die Mindestspeicherdauer von sechs Monaten hinausgegangen werden soll. Der von der Richtlinie vorgegebene Spielraum von bis zu 24 Monaten wird also nicht ausgeschöpft werden. Auch heute schon können Unternehmen nach dem Telekommunikationsgesetz Daten bis zu sechs Monate lange aufbewahren, um sie zur Rechnungslegung verwenden zu können. Diese Daten dürfen auch heute schon nach §§ 100g 100h StPO mit richterlichem Beschluss für die Strafverfolgung, bspw. bei der Verbreitung von kinderpornographischer oder fremdenfeindlicher Inhalte im Internet, herangezogen werden. Mit der Neuregelung ist allerdings auch eine Ausweitung des Datenpools verbunden, denn Standortdaten, IP- Adressen und E-Mail-Verbindungsdaten waren zu Abrechnungszwecken bislang nicht erforderlich.

Was sich außerdem ändert, ist Folgendes: aus der Erlaubnis für Unternehmen zur Speicherung von Daten wird durch die europäische Richtlinie eine Verpflichtung. In der Praxis bedeutet dies, dass die Unternehmen, die schon heute in der Regel drei Monate speichern, diesen Zeitraum um lediglich drei Monate verlängern müssen.

- **Speicherzweck und Datenabfrage** sind auf Zwecke der Strafverfolgung, d.h. die Ermittlung, Aufdeckung und Verfolgung von Straftaten von erheblicher Bedeutung beschränkt. Neu ist, dass Straftaten, die im Höchstmaß mit weniger als fünf Jahren Freiheitsstrafe bedroht sind, aus dem Straftatenkatalog gestrichen sind. Gleiches gilt für Straftaten, die mittels Telekommunikation begangen wurden, bspw. Urheberrechtsverletzungen durch illegalen Download. Wirtschaftskriminalität, Kriegsverbrechen, Menschenhandel, Kinderpornographie wurden neu in den Katalog aufgenommen. Die Tat muss - das ist ebenfalls neu – auch im konkreten Einzelfall schwer wiegen.

Für diese Daten muss ein tatsächlicher Bedarf vorliegen, und die Speicherung darf keinen unverhältnismäßigen Aufwand verursachen. Geprüft werden muss, ob die Aufklärung eines Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre. Zudem muss die Datenerhebung in angemessenem Verhältnis zur Bedeutung der Sache stehen.

Die Zweckbestimmung der Datenspeicherung ist trotz dieser Vorgaben sehr allgemein und definiert, weil Daten pauschal und ohne konkreten Verdachtsmoment gespeichert werden. Die Einbeziehung aller Teilnehmer und Netze bedingt zudem eine hohe Eingriffsintensität.

Die USA verfolgen zur Kommunikationsermittlung einen anderen Ansatz, das sog. "Quick Freeze". Es wird in begründeten Verdachtsfällen eingesetzt: Auf richterlichen Beschluss erfolgt dann eine Sicherung der Telekommunikationsdaten des jeweiligen Verdächtigen. Es kommt also zu einer individuellen, anlassbezogenen Speicherung.

- **Schutz des Kernbereichs privater Lebensgestaltung** (§ 100a Abs. 4 StPO): Als Zielobjekt kommt nur der vom Beschuldigten benutzte Anschluss in Frage. Eine Überwachung ist unzulässig, wenn ausschließlich Kernbereichserkenntnisse erlangt würden. Wenn trotzdem Erkenntnisse aus diesem Bereich ermittelt wurden, dürfen sie nicht verwertet werden und müssen unverzüglich gelöscht werden. Die Anordnung einer Überwachung bedarf also zusätzlich immer der Prognose, dass nicht allein Erkenntnisse aus dem Kernbereich zu erwarten sind.
- **Standort- und Verbindungsdaten**, wie Telefonnummern von Handys und Festnetzgeräten, werden nur für den Beginn des Mobilfunkverkehrs, nicht auch für das Ende gespeichert. Erfolgreiche Anrufversuche werden nicht aufgezeichnet. Es werden lediglich Internet-Einwahldaten, d.h. die IP- Adresse und der Einwahlzeitpunkt, sowie Verkehrsdaten zu Emails und Internettelefonie aufgezeichnet. Inhalte der vom Nutzer aufgerufenen Seiten und der Kommunikation werden ausdrücklich nicht protokolliert. Die Neuregelung sieht vor, diese Daten vielen Behörden zum Online-Abruf zur Verfügung zu stellen. Dazu gehören Polizei, Staatsanwaltschaft, Nachrichtendienste, Zoll und der Bundesanstalt für Finanzdienstleistungsaufsicht, kurz BaFin.

Datenschutzrechtliche Bedenken bestehen allerdings, wenn Nutzer öffentlich zugänglicher E-Mail-Dienste zur Angabe ihres Namens und ihrer Adresse verpflichtet werden.

- Für alle verdeckten Ermittlungsmaßnahmen gilt eine Reihe **grundrechtssichernder Verfahrensregelungen**. Dazu zählt etwa:
 - Höchstdauer der (Erst-/Verlängerungs-)Anordnung max. 3 Monate;

- nachträgliche Benachrichtigung der von verdeckten Ermittlungsmaßnahmen betroffenen Personen;
 - die Möglichkeit eines nachträglichen gerichtlichen Rechtsschutzes;
 - die Pflicht zur Löschung der aus verdeckten Ermittlungsmaßnahmen erlangten Erkenntnisse, sobald diese für Zwecke der Strafverfolgung sowie für einen etwaigen gerichtlichen Rechtsschutz nicht mehr erforderlich sind.
- **Schutz bei Berufsgeheimnisträgern (§ 160a StPO):** Wenn Erkenntnisse zu erwarten sind, die unter das Zeugnisverweigerungsrecht fallen, trifft das Gesetz eine Unterscheidung zwischen Geistlichen, Strafverteidigern und Abgeordneten einerseits und Rechtsanwälten, Ärzten, Steuerberatern, Notaren, Journalisten und Therapeuten andererseits.

Bei ersteren ist die Telekommunikationsüberwachung unzulässig. Das Vertrauensverhältnis zu Seelsorgern, Strafverteidigern und Abgeordneten wird absolut geschützt. Sie sind aufgrund ihrer besonderen verfassungsrechtlichen Stellung von allen strafprozessualen Ermittlungsmaßnahmen ausgenommen, die sich auf die Informationen beziehen, die ihnen in ihrer Eigenschaft als Berufsgeheimnisträger anvertraut wurden.

Letztere genießen nur einen relativen Schutz, d.h. hier erfolgt im Einzelfall vor Durchführung einer Ermittlungsmaßnahme eine **Abwägung zwischen Strafverfolgungs- und Geheimhaltungsinteresse**. Diese Abwägung gilt auch hinsichtlich der Nutzung von Erkenntnissen, die im Rahmen einer Ermittlungsmaßnahme gewonnen wurden.

Das BVerfG hat sich 2004 in einem Urteil zur akustischen Wohnraumüberwachung (1 BVR 273/98) zum Schutz von Berufsgeheimnisträgern geäußert: Die Überwachung muss unterbleiben, wo eventuell der Schutz der Menschenwürde oder des Kernbereichs der privaten Lebensführung der überwachten Person berührt wird. Da eine Einstufung einer entsprechenden Information allerdings erst nach Erhebung dieser Daten möglich ist, müssen vor Beginn der Überwachungsmaßnahme konkrete Anhaltspunkte dafür vorgelegt werden, dass das Gespräch nicht den privaten Bereich betrifft. Ein Anhaltspunkt für ein privates Gespräch kann aber die Anwesenheit eines Berufsgeheimnisträgers, wie eines Geistlichen, Strafverteidigers oder eines Arztes, sein. Dies kann also in Widerspruch zu einer Abwägung zwischen Strafverfolgungsinteresse und Grundrechtsschutz vor Einleitung der Ermittlungsmaßnahme stehen.

Für diese Abwägung definiert das Gesetz **Maßstäbe**. Ein Strafverfolgungsinteresse ist nur dann gegeben, wenn das Verfahren eine Straftat von erheblicher Bedeutung betrifft. Dies ist dann der Fall, wenn sie:

- mindestens dem Bereich der mittleren Kriminalität zugerechnet werden kann,
- den Rechtsfrieden empfindlich stört und
- dazu geeignet ist, das Gefühl der Rechtssicherheit der Bevölkerung erheblich zu beeinträchtigen.

Diese Relativierung der Zeugnisverweigerungsrechte stellt allerdings bei Journalisten eine Einschränkung des Informantenschutzes und des Redaktionsgeheimnisses dar. Denn die Kommunikation zwischen Journalisten und ihren Quellen genießt verfassungsrechtlich garantierten Schutz.

Nach heutiger Rechtslage gilt: soweit das Zeugnisverweigerungsrecht der Journalisten reicht, ist die Beschlagnahme von Schriftstücken, Ton-, Bild- und Datenträgern usw., die sich in ihrem Gewahrsam befinden, unzulässig (§ 97 Absatz 5 StPO). Zur Sicherstellung und Beschlagnahme von Unterlagen, die bei Journalisten gefunden wurden und auf einen Geheimnisverrat durch eine noch unbekannte Person hindeuteten, wurden in der Vergangenheit daher oftmals Journalisten der Beihilfe zum Geheimnisverrat verdächtigt. (vgl. Cicero- Fall) Mit der neuen Vorschrift wird die Verwertung solcher Unterlagen zu Beweiszecken nun ausgeschlossen.

Besteht gegen den Berufsgeheimnisträger, etwa einen Journalisten, selbst ein Beteiligungs- oder Begünstigungsverdacht, so können nach geltendem Recht Unterlagen bei ihm beschlagnahmt werden, wenn diese für die Aufklärung einer Straftat relevant sind (sog. **Verstrickungsfälle**). Auch für diese Verstrickungsfälle soll zukünftig die Verwertung von sog. Zufallsfunden entweder ganz ausgeschlossen oder zumindest erschwert werden. Zufallsfunde sind solche Beweismittel, die in keinem Zusammenhang mit dem der Durchsuchung zugrunde liegendem Verfahren stehen und sich nicht auf eine schwere Straftat (Höchstmaß mindestens fünf Jahre Freiheitsstrafe) oder Geheimnisverrat beziehen. Damit sind Delikte im Bereich der kleinen und mittleren Kriminalität letztendlich ausgeschlossen.