**Marius Wallmeier**

# Telekommunikationsüberwachung als verdeckte polizeiliche Maßnahme der Strafprozessordnung

**Bachelorarbeit**

# Telekommunikationsüberwachung als verdeckte polizeiliche Maßnahme der Strafprozessordnung

Fachbereich: Polizeivollzugsdienst
Hochschule: Fachhochschule für öffentliche Verwaltung des Landes Nordrhein- Westfalen

Bachelor-Thesis

## Gliederung

# Literaturverzeichnis:

## I. Kommentare:


Hrsg. von Büchner, Wolfgang / Bönsch, Georg
**Beck`scher TKG Kommentar**
2. Auflage, 2000, München

Eisenberg, Ulrich
**Beweisrecht der StPO – Spezialkommentar**
7. Auflage, 2011, München

Hrsg. von Hannich, Rolf
**Karlsruher Kommentar zur Strafprozessordnung**
6. Auflage, 2008, München

Jarass, Hans D. / Pieroth, Bodo
**Grundgesetz für die Bundesrepublik Deutschland**
11. Auflage, 2011, München

Löwe, Ewald / Erb, Volker
**Die Strafprozessordnung und das Gerichtsverfassungsgesetz**
26. Auflage, 2006-2010, Berlin

Meyer-Goßner, Lutz
**Strafprozessordnung mit GVG und Nebengesetzen**
53. Auflage, 2010, München

Rudolphi, Hans-Joachim
**Systematischer Kommentar zum Strafgesetzbuch**
Loseblattsammlung
Frankfurt am Main


## II. Lehrbücher:


Beulke, Werner
**Strafprozessrecht**
11. Auflage, 2010, Heidelberg

Beulke, Werner / Ruhmanseder, Felix
**Die Strafbarkeit des Verteidigers**
2. Auflage, 2010, Heidelberg

Detterbeck, Steffen
**Öffentliches Recht**
8. Auflage, 2011, München

Kay, Wolfgang
**Allgemeines Verwaltungs- und Eingriffsrecht im Polizeidienst**
**Band I - Grundlagen -**
8. Auflage, 2009, Witten

Keller, Christoph
**Telekommunikationsüberwachung und andere verdeckte Ermittlungsmaßnahmen**
1. Auflage, 2008, Stuttgart

Larenz, Karl / Canaris, Claus-Wilhelm
**Methodenlehre der Rechtswissenschaft**
3. Auflage, 1995, Berlin

Löffelmann, Dr. Markus / Walther, Alexander / Reitzenstein, Robert Frank
**Das strafprozessuale Ermittlungsverfahren**
1. Auflage, 2007, Bonn

Malek, Klaus / Wohlers, Wolfgang
**Zwangsmaßnahmen und Grundrechtseingriffe im Ermittlungsverfahren**
2. Auflage, 2001, Heidelberg

Roxin, Claus / Schünemann, Bernd
**Strafverfahrensrecht**
26. Auflage, 2009, München

Schröder, Burkhard / Schröder Claudia
**Die Online-Durchsuchung**
**Rechtliche Grundlagen, Technik, Medienecho**
1. Auflage, 2008, Hannover

Seitz, Nicolai
**Strafverfolgungsmaßnahmen im Internet**
1. Auflage, 2004, Köln

Tetsch, Lambert Josef
**Eingriffsrecht**
**Band 1: Grundlagen und Datenverarbeitung**
4. Auflage, 2008, Hilden

## III. Zeitschriften:

Allgayer, Peter
**Die Verwendung von Zufallserkenntnissen aus *Überwachung der Telekommunikation gem. §§ 100a StPO (und anderen ermittlungsmaßnahmen)**
In: NStZ 2006, 603

Artkämper, Heiko
**Ermittlungen in Funktelefonnetzen**
In: Kriminalistik 1998, 202

Baldus, Prof. Dr. Manfred
**Der Kernbereich privater Lebensgestaltung – absolut geschützt, aber abwägungsoffen**
In: JZ 2008, 218

Bär, Wolfgang
**Telekommunikationsüberwachung und andere verdeckte Ermittlungsmaßnahmen – Gesetzliche Neuregelungen zum 1.1.2008**
In: MMR 2008, 215

Bär, Wolfgang
**Beschlagnahme von Computerdaten (I)**
In: CR 1996, 675

Bär, Wolfgang
**Beschlagnahme von Computerdaten (II)**
In: CR 1996, 744

Barton, Prof. Dr. Stephan
**Annmerkung: Freiheit der Kommunikation zwischen Verteidiger und Beschuldigtem**
In: JZ 2010, 102

Becker, Dr. Christian / Meinicke, Dirk
**Die so genannte Quellen-TKÜ und die StPO – Von einer „herrschenden Meinung“ und ihre fragwürdigen Entstehung**
In: StV 2011, 50

Beichel-Benedetti, Stephan
**Anordnung einer sogenannten Funkzellenabfrage bei einem Telekommunikationsanbieter**
In: StV 2005, 438

Beulke, Werner / Ruhmannseder, Felix
**Strafprozessuale Zwangsmaßnahmen in der Verteidigungssphäre (Teil 1)**
In: StV 2011, 180

Beulke, Werner / Ruhmannseder, Felix
**Strafprozessuale Zwangsmaßnahmen in der Verteidigungssphäre (Teil 2)**
In: StV 2011, 252

Böckenförde, Dr. Thomas
**Auf dem Weg zur elektronischen Privatsphäre**
In: JZ 2008, 925

Bosch, Prof. Dr. Nikolaus
**Verwertung von Telekommunikationsverbindungsdaten**
In: JA 2006, 747

Braum, Dr. Stefan
**Expansive Tendenzen der Telekommunikations-Überwachung?**
In: JZ 2004, 128

Breyer, Dr. Patrick
**Rechtsprobleme der Richtlinie 2006/24/EG zur Vorratsdatenspeicherung und ihrer Umsetzung in Deutschland**
In: StV 2007, 214

Brodowski, Dominik
**Strafprozessualer Zugriff auf E-Mail-Kommunikation**
In: JR 2009, 402

Burchhard, Dirk
**Verfassungsrechtliche Interessenabwägung im Informationsrecht**
In: KritV 1999, 239

Demko, Dr. Daniela
**Die Erstellung von Bewegungsbildern mittels Mobiltelefon als neuartige strafprozessuale Observationsmaßnahme.**
In: NStZ 2004, 57

Eisenberg, Dr. Ulrich / Nischan, Anett
**Strafprozessualer Zugriff auf digitale multimediale Videodienste**
In: JZ 1997, 74

Eckhardt, Jens
**Die Neuregelung der Telekommunikationsüberwachung und andere verdeckter Ermittlungsmaßnahmen**
In: CR 2007, 336

Füllkrug, Michael
**Telefonüberwachung als kriminalistische Erkenntnisquelle**
In: Kriminalistik 1990, 349

Gercke, Dr. Björn
**Rechtliche Probleme durch den Einsatz des IMSI-Catchers**
In: MMR 2003, 453

Göres, Ulrich
**Rechtmäßigkeit des Zugriffs der Strafverfolgungsbehörden auf die Daten der Mauterfassung**
In: NJW 2004, 195

Götz, Hansjörg
**Sicherstellung von Mobiltelefonen**
In: Kriminalistik 2005, 300

Gusy, Christoph
**Lauschangriff und Grundgesetz**
In: JuS 2004, 457

Glaser, Michael / Gedeon, Bertolt
**Dissonante Harmonie: Zu einem zukünftigen „System“ strafprozessualer verdeckter Ermittlungsmaßnahmen**
In: GA 2007, 415

Heintschel-Heinegg; Prof. Dr. Bernd
**IMSI-Catcher**
In: JA 2007, 75

Henrichs, Axel
**TKÜ-Maßnahmen und andere Intensivermittlungen**
In: Kriminalistik 2008, 169

Hoeren, Prof. Dr. Thomas
**Die Umsetzung der Richtlinie zur Vorratsdatenspeicherung – Konsequenzen für die Privatwirtschaft**
In: JZ 2008, 668

Hilger, Dr. Hans
**Gesetzgebungsbericht: Über den neuen § 100i StPO**
In: GA 2002, 557

Hornung, Dr. Gerrit
**Ein neues Grundrecht**
In: CR 2008, 299

Jahn, Prof. Dr. Matthias
**Der strafprozessuale Zugriff auf Telekommunikationsverbindungsdaten – BVerfG, NJW 2006, 976**
In: JuS 2006, 491

Joecks, Dr. Wolfgang
**Die strafprozessuale Telefonüberwachung**
In: JA 1983, 59

Keller, Christoph
**Überwachung des E-Mail-Verkehrs und „Online-Streife“**
In: Kriminalistik 2009, 491

Kinzig, Prof. Dr. Jörg
**Die Telefonüberwachung in Verfahren organisierter Kriminalität: Fehler bei der richterlichen Anordnung, Mängel des Gesetzes.**
In: StV 2004, 560

Knierim, Thomas C.
**Fallrepetitorium zur Telekommunikationsüberwachung nach neuem Recht**
In: StV 2008, 599

Kretschmer, Dr. Joachim
**Die Verwertung sogenannter Zufallsfunde bei der strafprozessualen Telefonüberwachung**
In: StV 1999, 221

Kudlich, Dr. Hans
**Der heimliche Zugriff auf Daten in einer Mailbox: Ein Fall der Überwachung des Fernmeldeverkehrs? – BGH, NJW1997, 1934**
In: JuS 1998, 209

Kudlich, Dr. Hans
**Geldwäscheverdacht und Überwachung der Telekommunikation**
In: JR 2003, 453

Küpper, Dr. Herbert
**Tagebücher, Tonbänder, Telefonate.**
In: JZ 1990, 416

Leutheusser-Schnarrenberger, Sabine
**Vorratsdatenspeicherung – Ein vorprogrammierter Verfassungskonflikt**
In: ZRP 2007, 9

Lepsius, Dr. Oliver
**Der große Lauschangriff vor dem Bundesverfassungsgericht (Teil I).**
In: Jura 2005, 433

Lepsius, Dr. Oliver
**Der große Lauschangriff vor dem Bundesverfassungsgericht (Teil II).**
In: Jura 2005, 586

Löffelmann, Dr. Markus
**Die Übertragbarkeit der Judikatur des Bundesverfassungsgerichts zur akustischen Wohnraumüberwachung auf die Telekommunikationsüberwachung und andere verdeckte Ermittlungsmaßmaßnahmen**
In: ZStW 2006, 358

Maiwald, Prof. Dr. Manfred
**Zufallsfunde bei zulässiger strafprozessualer Telefonüberwachung – BGH, NJW 1976, 1462**
In: JuS 1978, 379

Mosbacher, Dr. Andreas
**Aktuelles Strafprozessrecht**
In: JuS 2008, 125

Müssig, Dr. Bernd
**Beweisverbote im Legitimationszusammenhang von Strafrechtstheorie und Strafverfahren**
In: GA 1999, 119

Palm, Franz / Roy, Rudolf
**Mailboxen: Staatliche Eingriffe und andere rechtliche Aspekte**
In: NJW 1996, 1791

Palm, Franz / Roy, Rudolf
**Der BGH und der Zugriff auf Mailboxen**
In: NJW 1997, 1904

Puschke, Dr. Jens / Singelnstein, Tobias
**Telekommunikationsüberwachung, Vorratsdatenspeicherung und (sonstige) heimliche Ermittlungsmaßnahmen der StPO nach der Neuregelung zum 1.1.2008**
In: NJW 2008, 113

Rogall, Prof. Dr. Klaus
**Beweiserhebungs- und Beweisverwertungsverbote im Spannungsfeld zwischen den Garantien des Rechtsstaates und der effektiven Bekämpfung von Kriminalität und Terrorismus.**
In: JZ 2008, 818

Roggan, Prof. Dr. Frederik
**Das neue BKA-Gesetz – Zur weiteren Zentralisierung der deutschen Sicherheitsarchitektur**
In: NJW 2009, 257

Ruthig, Dr. Josef
**Die Unverletzlichkeit der Wohnung (Art. 13 GG n.F.)**
In: JuS 1998, 506

Ruhmannseder, Dr. Felix
**Die Neuregelung der strafprozessualen verdeckten Ermittlungsmaßnahmen**
In: JA 2009, 57

Sankol, Barry
**Strafprozessuale Zwangsmaßnahmen und Telekommunikation**
In: JuS 2006, 698

Sankol, Barry
**Überwachung und Internet – Telefonie**
In: CR 2008, 13

Schatzschneider, Prof. Dr. Wolfgang
**Telefondatenverarbeitung und Fernmeldegeheimnis**
In: NJW 1993, 2029

Schroth, Prof. Dr. Ulrich
**Beweisverwertungsverbote im Strafverfahren – Überblick, Strukturen und Thesen zu einem umstrittenen Thema**
In: JuS 1998, 969

Sehr, Peter
**INPOL - neu: System mit Merkmalen eines extremen Wandels**
In: Kriminalistik 1999, 532

Simitis, Prof. Dr. Spiros
**Die informationelle Selbstbestimmung – Grundbedingung einer verfassungskonformen Informationsordnung**
In: NJW 1984, 398

Singelnstein, Tobias
**Strafprozessuale Verwendungsregelungen zwischen Zweckbindungsgrundsatz und Verwertungsverboten. Voraussetzungen der Verwertung von Zufallsfunden uns sonstiger zweckentfremdeter Nutzung personenbezogener Daten im Strafverfahren seit dem 1. Januar 2008**
In. ZStW 2008, 854

Singelnstein, Dr. Tobias
**Rechtschutz gegen heimliche Ermittlungsmaßnahmen des § 101 VII 2-4 StPO**
In: NStZ 2009, 481

Thiede, Frank
**Das Auslesen von beschlagnahmten Mobilfunkgeräten**
In: Kriminalistik 2005, 346

Thiede, Frank
**Gerätekennung eines Handys als Anknüpfungspunkt für Telekommunikationsüberwachung**
In: Kriminalistik 2003, 165

Valerius, Dr. Brian
**Ermittlungsmaßnahmen im Internet**
In: JR 2007, 275

Vassilaki, Dr. Irini E.
**Die Überwachung des Fernmeldeverkehrs nach der Neufassung der §§ 100a, 100b StPO Erweiterung von staatlichen Grundrechtseingriffen**
In: JR 2000, 446

Welp, Dr. Jürgen
**Verbindungsdaten. Zur Reform des Auskunftsrechts (§100g, 100h StPO)**
In: GA 2002, 535

Wollweber, Dr. Harald
**Nochmals: Das Strafänderungsgesetz 1999**
In: NJW 2000, 3623

Wolter, Dr. Jürgen
**Alternativen zum Regierungs-Entwurf 2007 zur Neuregelung der Ermittlungsmaßnahmen – Heike Jung zum 65. Geburtstag**
In: GA 2007, 183

Zöller, Dr. Mark Alexander
**Verdachtslose Recherche und Ermittlung im Internet**
In: GA 2000, 563

Zöller, Prof. Dr. Mark Alexander
**Vorratsdatenspeicherung zwischen nationaler und europäischer Strafverfolgung**
In: GA 2007, 393

## IV. Online - Zeitschriften:

Burghardt, Boris
**Die neue Unübersichtlichkeit – Rechtsprechung des BGH zum nachträglichen Rechtsschutz gegen verdeckte Ermittlungsmaßnahmen**
In: HRRS 2009, 567
*Internetzeitung für Strafrecht – www.hrr-strafrecht.de*

Buermeyer, Ulf
**Die „Online-Durchsuchung".**
**Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme**
In: HRRS 2007, 154
*Internetzeitung für Strafrecht – www.hrr-strafrecht.de*

Buermeyer,, Ulf
**Zur Rechtswidrigkeit der Quellen-Telekommunikationsüberwachung auf Grundlage des § 100a StPO**
In: HRRS 2009, 433
*Internetzeitung für Strafrecht – www.hrr-strafrecht.de*

Deiters, Mark; Albrecht, Anna Helena
**BVerfG, Urteil vom 27.2.2008 – 1 BvR 370/07; 1 BvR 595/07**
In: ZJS 2008, 319
*Zeitschrift für das Juristisch Studium – www.zjs-online.com*

Gaede, Karsten
**Schlechtverteidigung – Tabus und Präklusionen zum Schutz vor dem Recht auf wirksame Verteidigung?**
In: HRRS 2007, 402
*Internetzeitung für Strafrecht – www.hrr-strafrecht.de*

Harnisch, Stefanie; Pohlmann, Martin
**Strafprozessuale Maßnahmen bei Mobilfunkendgeräten**
In: HRRS 2009, 202
*Internetzeitung für Strafrecht – www.hrr-strafrecht.de*

Korn, Jana
**Der strafprozessuale Zugriff auf Verkehrsdaten nach § 100g StPO**
In: HRRS 2009, 112
*Internetzeitung für Strafrecht – www.hrr-strafrecht.de*

Schlegel, Stephan
**„Beschlagnahme“ von E-Mail-Verkehr beim Provider**
In: HRRS 2007, 44
*Internetzeitung für Strafrecht – www.hrr-strafrecht.de*

Schlegel, Stephan
**„Online-Durchsuchung-light“**
**Die Änderungen des § 110 StPO durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung**
In: HRRS 2008, 23
*Internetzeitung für Strafrecht – www.hrr-strafrecht.de*

## V. Internet - Quellen:

http://www.bundesjustizamt.de
(Zahlen der Telekommunikationsüberwachung für 2009)

## VI. Sonstige - Quellen:

Jordan, Stefan
**Einsatz des MAC-Catchers zum W-LAN Scannen, rechtliche Einsatzmöglichkeiten bei der Strafverfolgung**
In: Recht und Polizeipraxis, Wiesbaden 21.09.2005
Bundekriminalamt KI 15

Prantl, Heribert
**Die große Niederlage des Verfassungsgerichts**
In: Süddeutsche Zeitung vom 2. Juli 2007, Nr. 149, Seite 4

Sparenberg, Philipp; Heintz, Veris-Pascal
**Online - Durchsuchung und Vorratedatenspeicherung**
**Das neue BKA-Gesetz – mit Vollgas in den Überwachungsstaat**
In: Freilaw – Freiburg Law Students Journal Ausgabe 2/2009

## Abkürzungsverzeichnis:

| | |
|---|---|
| BtM | Betäubungsmittel |
| GG | Grundgesetz |
| IMEI | International Mobile Equipment Identity |
| IMSI | International Mobile Subscriber Identity |
| MAC | Media Access Control |
| MMS | Multimedia Messaging Service |
| PC | Personal Computer |
| SMS | Short Message Service |
| SIM | Subscriber Identity Module |
| StPO | Strafprozessordnung |
| TKG | Telekommunikationsgesetz |
| TKÜ | Telekommunikationsüberwachung |
| TKÜV | Telekommunikationsüberwachungsverordnung |
| VoIP | Voice over Internet Protocol |
| W-LAN | Wireless Local Area Network |

# Telekommunikationsüberwachung als verdeckte polizeiliche Maßnahme der Strafprozessordnung

## 1 Einleitung

Telekommunikationsüberwachung ist eine im Strafverfahrensrecht und Polizeirecht gängige Bezeichnung für die Überwachung von Telekommunikationsvorgängen mit dem Ziel der Feststellung von Kommunikationsinhalte und Kommunikationsdaten. Darunter fallen die Aufzeichnung von Gesprächen und das Auslesen von E-Mails, Kurzmitteilungen in der Form von SMS und MMS sowie Telefax.

Die Möglichkeit der gezielten Überwachung der modernen Telekommunikation ist durch das G 10, auch Abhörgesetz genannt, eröffnet worden.[1] Die Überwachung der Telekommunikation ist eine verdeckte Ermittlungsmaßnahme der Strafprozessordnung und ist in einer Reihe von Vorschriften geregelt, die auf komplexe Weise ineinander greifen und deren jeweiliger Anwendungsbereich mitunter schwer abzugrenzen ist. Die Telekommunikationsüberwachung im Rahmen des Strafverfahrens wurde in § 100a ff. StPO geregelt.[2] Hinzu treten noch die Vorschriften des Telekommunikationsgesetztes und die der Telekommunikations-Überwachungsverordnung.

Die Rechtsfolgen von § 100a StPO gehen über die bloße Wahrnehmung von Gesprächsinhalten hinaus und erfassen ebenfalls auch die entstehenden Daten des technischen Vorganges bei dem jeweiligen Kommunikationsereignis. Insofern erfolgt ein universaler Zugriff auf die persönliche Sphäre des Einzelnen, deren Schutz aus dem Grundgesetz hergeleitet wird.

Betroffen sind hier vor allem Art. 10 und 13 GG, ebenso die informationeller Selbstbestimmung, die aus Art. 2 I 1 I GG abgeleitet wird.[3]

Grundgesetzlich wird bei dem Fernmeldegeheimnis im Sinne des Art. 10 GG die gesamte individuelle Kommunikation über das Medium der drahtlosen oder drahtgebundenen elektromagnetischen Wellen vor dem Zugriff der öffentlichen Gewalt geschützt. Der Schutz umfasst vor allem den Telefon-, Telegramm-, Funk-, Teletext-, Telefaxverkehr und Bildschirmdienst, aber auch die Kommunikation über das Internet.

Eingriffe in Art 10 I GG liegen vor, wenn die öffentliche Gewalt vom Inhalt oder den Daten der Sendungen oder Mitteilungen Kenntnis nimmt, sowie die Speicherung diesbezüglich erlangter Informationen, deren Verwertung und Weitergabe vornimmt.[4]

---

[1] KK-Pfeifer / Hannich, Einl., Rn.32e.
[2] Historisch: Löffelmann / Walther / Reitzenstein, §3, Rn. 21.
[3] Vgl. Glaser / Gedeon, GA 2007, 415ff..
[4] BVerfGE 106, 28; Detterbeck, ÖR, Rn. 701f.; BVerfGE 113, 348.

In den Schutzbereich des Art. 13 I GG fällt die Wohnung. Wohnung im Sinne des Grundrechts sind alle Räume, die der allgemeinen Zugänglichkeit durch eine räumliche Abschottung entzogen und zur Stätte privaten Lebens und Wirkens gemacht sind.[5]
Eingriffe liegen bei allen staatlichen Maßnahmen vor, die die Privatheit der Wohnung ganz oder teilweise aufheben. In Betracht kommt in erster Linie körperliches Eindringen durch die staatliche Gewalt wie auch unkörperliches Eindringen mittels technischer Hilfsmittel.[6]
Das Recht auf informationelle Selbstbestimmung im Sinne des Art. 2 I i.V.m. Art 1 I GG ist sehr weit gefasst. Es schützt umfassend das Recht des Einzelnen über die Preisgabe und die Verwendung seiner personenbezogenen Daten zu bestimmen.[7] Eingriffe in dieses Grundrecht können somit sehr vielfältig sein. So hat das BVerfG jüngst aus dem allgemeinen Persönlichkeitsrecht aus Art 2 I i.V.m. Art. 1 I GG eine neue Schutzdimension geschaffen, mit der die Integrität und die Vertraulichkeit des eigengenutzten informatorischen Systems geschützt wird, das sogenannte IT-Grundrecht.[8] Inhaltlich weist dieses Grundrecht zwei unabhängige Schutzgehalte aus, denn es richtet sich gegen Verletzungen der Integrität ebenso wie der Vertraulichkeit des informatorischen Systems. Das IT-Grundrecht schützt somit umfassend jedes informatorische System, der Schutzgegenstand wurde sehr weit formuliert.[9]
Wie schon die vorstehend angeführte Entscheidung des BVerfG zeigt, sind in dem komplexen Gebiet des Rechts stetige Veränderungen festzustellen und durch die Ermittlungsbehörden zu berücksichtigen. Diese Veränderungen treten nicht nur an den bestehenden Gesetzen, sondern gerade auch in Bezug auf die Gesetzesanwendung und der Auslegung durch die Rechtsprechung auf.
Die Definition eines einzelnen Begriffes kann schon für die polizeiliche Ermittlungsarbeit von großer Bedeutung sein. Einen nicht zu vernachlässigenden Einfluss hat auch die Tatsache, dass Europa in rechtlichen Fragen näher zusammenrückt und so nicht nur in Deutschland selbst Einfluss auf die Gestaltung rechtlicher Fragen im Bereich der Telekommunikationsüberwachung genommen wird. So mussten in der Vergangenheit die Vorgaben des Übereinkommens über Computerkriminalität des Europarates[10] und die Richtlinie 2006/24/EG[11] in nationales Recht umgesetzt werden.[12]
Im Lichte all dieser Aspekte ist überdies zu berücksichtigen, dass jedes überwachte Telefonat einen tiefen Grundrechtseingriff darstellt. Befürchtungen auf Seiten der Bürger und Datenschützer, dass sich Deutschland in Richtung eines Überwachungsstaates entwickelt,

[5] Detterbeck, ÖR, Rn. 766; Gusy, JuS 2004, 457; Lepsius, Jura 2005, 433 und 586.
[6] Jarass / Pieroth, Art. 13, Rn.4f..
[7] Simitis, NJW 1984, 398; Burchard, KritV 1999, 239 m.w.N..
[8] Hierzu vertiefend: Deiters / Albrecht, ZJS 2008, 319.
[9] Hornung, CR 2008, 299; Buermeyer, HRRS 2009, 433.
[10] Cybercrime-Konvention (vom 23.11.2001, European Treaties Series No. 185).
[11] Leutheusser-Schnarrenberger, ZRP 2007, 9ff; Breyer, StV 2007, 214ff.; Wolter, GA 2007, 183ff..
[12] BT-Drucks. 16/5846; BT-Drucks.16/6979 ;BVerfG, NJW 2005; 1338; 2005, 1637; 2006, 976; siehe hierzu auch: Löffelmann / Walther / Reitzenstein, §3, Rn. 1.

sind auf Grund der stetig steigenden Anzahl von Überwachungsanordnungen erklärbar. Insbesondere die Heimlichkeit der Überwachung und die mit der Überwachung verbundene Gefahr , dass in den unantastbaren Kernbereich der privaten Lebensgestaltung[13] eingegriffen werden könnte, führt dazu, dass der Focus der Öffentlichkeit hierauf gerichtet ist und die Maßnahmen bisweilen heftig kritisiert und deren Rechtmäßigkeit in Frage gestellt werden.[14]

Im Bereich der Gefahrenabwehr gibt es in Nordrhein Westfalen für die Telekommunikationsüberwachung keine Regelungen. In einigen anderen Bundesländern[15] sind Regelungen für eine präventive, gefahrenabwehrende Telekommunikationsüberwachung getroffen worden. Ein bedeutender Anwendungsbereich der präventiven Telekommunikationsüberwachung ergibt sich in der Regel aus Gemengelagen, kennzeichnend hierfür ist, dass der Polizeieinsatz sowohl repressive als auch präventive Zielrichtungen hat.[16] Die Strafverfolgungsbehörden in NRW können bisher lediglich nach § 100a StPO vorgehen und müssen eine, wie nachfolgend noch näher erläutert wird, rechtlich umstrittene Umwidmung der erlangten Daten vornehmen.

In der Strafprozessordnung finden sich die Vorschriften, die die Polizei betreffen und die Speicherung und Nutzung von personenbezogenen Daten regeln in §§ 483-486 und § 489 StPO. Ergänzt werden die Regelungen in § 24 II PolG NRW.

Da keine Zweckidentität zwischen Strafverfolgung und Gefahrenabwehr besteht, die Aufgabenbereiche unterschiedlich sind, ist die Norm als Umwidmungserlaubnis anzusehen.[17] Die Nutzung personenbezogener Daten, die aus Maßnahmen Strafverfolgungsmaßnamen stammen, ist nur unter strengen Voraussetzungen der StPO möglich und werde durch polizeigesetzliche Regelungen weiter eingeschränkt.[18] Im Bereich der Telekommunikationsüberwachung ist die Umwidmung hauptsächlich nur möglich, zur Abwehr einer im Einzelfall bestehenden Gefahr für Leib oder Freiheit einer Person oder Gegenstände vom bedeutenden Wert.[19] Eine Umwidmung ist folglich an sehr strenge Voraussetzungen gekoppelt, die für jeden Einzelfall zu prüfen sind.

Standartfall der Umwidmung[20] dürfte die Nutzung der erlangten Daten für die Verwendung in der Kriminalaktensammlung und die Verwendung im Rahmen des INPOL- Systems.

Ziel dieser Arbeit soll es sein, die strafprozessualen Regelungen näher zu betrachten und etwaige konfliktträchtige Konstellationen aufzuzeigen.

---

[13] Wolter, GA 2007, 183; Glaser / Gedeon, GA 2007, 415ff..
[14] Schröder / Schröder, Kapitel 3, S. 39ff. m.w.N..
[15] § 34a-c BayPAG; § 33 BdbPolG; § 10a-d HmbgDVG Pol; § 34a, b SOG MV; § 31 POG Rpl; § 33a Nds SOG.
[16] Vgl. Tetsch, Eingriffsrecht, Kapitel 5.1.2.13.2; Kay, Allg. VR, Bd. I, Kapitel, 6 S. 359f..
[17] Siehe hierzu: Tetsch, Eingriffsrecht, Kapitel 5.1.3.8, S. 458f..
[18] Wollweber, NJW 2000, 3623; Singelnstein, ZStW 2008, 854.
[19] Tetsch, Eingriffsrecht, Kapitel 5.1.3.8, S. 458f..
[20] Sehr, Kriminalistik 1999, 532; Tetsch, Eingriffsrecht, Kapitel 5.1.3.2, S. 383ff..

## 2 Statistik

Die Zahlen zur Telekommunikationsüberwachung werden seit Jahren durch die Staatsanwaltschaften erhoben und durch das Justizministerium veröffentlicht. Im Jahr 2009 wurden in ganz Deutschland 5.301 Maßnahmen, davon in NRW 526 Maßnahmen in Form der Telekommunikationsüberwachung gemäß § 100a StPO durchgeführt. Hauptsächlich wurde die Mobilfunktelekommunikation überwacht. Nur 51 Maßnahmen richteten sich auf die Überwachung der Internettelekommunikation.
Eine Telekommunikationsüberwachung gemäß § 100g StPO wurde im Jahre 2009 für ganz Deutschland 9.459 und davon in NRW 931 Mal angeordnet.[21]

## 3 Begriffsbestimmungen

Für die folgende Betrachtung ist es unumgänglich, ein einheitliches Begriffsverständnis zu schaffen. Daher sollen zunächst die Begriffe „Telekommunikation“ und „Überwachung und Aufzeichnung“ betrachtet und erläutert werden.

### 3.1 Telekommunikation

Bei der Einführung der Telefonüberwachung im Jahre 1968 hatte der Gesetzgeber die Möglichkeit der Überwachung analoger Festnetzanschlüsse im Sinn, die Vorstellung von Telekommunikation war geprägt von Telefon, Telefax und Fernschreiben. Seitdem haben sich nicht nur die rechtspolitischen Zielbestimmungen der Telekommunikationsüberwachung, sondern auch die technische Infrastruktur und die Marktbedingungen der Telefonie erheblich gewandelt. Das Begriffsspektrum der Telekommunikation[22] ist in den letzten Jahren vor allem durch die Möglichkeiten der Personal-Computer deutlich erweitert worden. Der Computer ist in den Rang eines Kommunikationsmediums aufgestiegen und stellt nicht mehr nur ein Gerät dar, mittels dessen Kommunikationsinhalte gespeichert und gesteuert werden können. So kann mit dem Computer telefoniert werden: **V**oice **o**ver **I**nternet **P**rotocol. Mit dem Mobiltelefon kann man im Internet surfen und E-Mails verschicken. Vom Computer kann man SMS und MMS auf Mobiltelefone versenden. Diese Veränderung des Begriffs der Telekommunikation kann auch an den Veränderungen des § 100a StPO festgemacht werden. So wurde aus der Telefonüberwachung die Überwachung der Telekommunikation. All diese Veränderungen zeigen, dass der Begriff Telekommunikation als solches nicht alleine an technischen Geräten festgemacht werden kann. Daher kommt der Legaldefinition des § 3 TKG eine besondere Bedeutung zu:[23]

---

[21] Zahlen von: http://www.bundesjustizamt.de/nn_1629916/DE/Themen/Justizstatistik/Telekommunikationsueberwachung/Telekommunikationsueberwachung_node.html?__nnn=true.
[22] Zöller, GA 2000, 563; Eisenberg / Nischan, JZ 97, 74.
[23] Siehe hierzu: Meyer-Goßner, §100a, Rn. 6; KK-Nack, § 100a, Rn. 4.

*„Telekommunikation ist der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen.*
*Telekommunikationsanlagen sind technische Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können“*

Durch diese abstrakte, technische Begriffsbestimmung wird nicht nur das technische Gerät als solches erfasst, vielmehr wird auch die Vernetzung von Geräten und die dadurch entstehende Telekommunikationsanlage erfasst. Es ist folglich nahezu jede Nachrichtenübermittlung vom Anwendungsbereich des § 100a ff. StPO umfasst.[24] Es werden also alle mit dem Versenden und Empfangen von Nachrichten mittels Telekommunikationsanlagen in Zusammenhang stehenden Vorgänge erfasst.

### 3.2 Überwachung und Aufzeichnung

In § 100a StPO wird von Überwachen und Aufzeichnen der Telekommunikation gesprochen. Der Begriff des Überwachens und Aufzeichnens ist in den einschlägigen Gesetzen und Verordnungen nicht legal definiert.
Sowohl das Überwachen als auch das Aufzeichnen muss gemäß § 100b I StPO durch einen Richter angeordnet werden, nur bei Gefahr in Verzug kann die Anordnung auch durch die Staatsanwaltschaft ergehen.[25]
Das Aufzeichnen und gegebenenfalls Speichern von Daten ist nicht in dem Begriff des Überwachens enthalten und muss als eine ergänzende Maßnahme zu der Grundmaßnahme, der Überwachung, mit angeordnet werden.[26]
Überwachen könnte im Licht des Art. 10 GG folgendermaßen definiert werden:

*„Überwachen meint, das sich zugänglich machen von Telekommunikationsdaten, die unter dem Schutz des Art. 10 GG stehen, durch staatliche Stellen. Wobei zugänglich machen das Lesen und Mithören ist.“*[27]

Im Rahmen dieser Arbeit soll unter TKÜ-Maßnahmen das Umleiten sowie Weiterleiten von Telekommunikationsdaten auf technische Speichermedien und das Abrufen von diesen verstanden werden. Es soll unter dem Aspekt eines umfassenden Eingriffs in Art. 10 GG und die allgemeinen Persönlichkeit- und Freiheitsrechte aus Art. 2 I GG betrachtet werden.

[24] Siehe hierzu Beulke, § 12 Rn. 253a; Kudlich, JuS1998, 209; BGH, NStZ 2003, 668.
[25] Meyer-Goßner, §100a, Rn. 8; §100b, Rn.3, 4;Löffelmann / Walther / Reitzenstein, §3, Rn. 24.
[26] Schatzschneider, NJW 1993, 2029.
[27] Vgl. Jarass / Pieroth, Art.10, Rn. 11; siehe auch : BVerfG, NJW 2003, 1787.

## 4 Rechtliche Betrachtung

Eine Telekommunikationsüberwachung stellt primär einen Eingriff in Art. 10 GG dar. Der Schutzbereich des Art. 10 GG garantiert die Unverletzlichkeit des Briefgeheimnisses, des Postgeheimnisses und des Fernmeldegeheimnisses.
Der Schutzbereich des Art. 10 GG erfasst demnach vier Aspekte der Kommunikation, nämlich:

a. den Kommunikationsinhalt;
b. die Umstände der Kommunikation;
c. die Bedingungen einer freien Telekommunikation;
d. die weiter Verwendung der durch Art. 10 GG geschützten Daten.[28]

In neueren Entscheidungen betont das BVerfG auch einen Menschenwürdegehalt des Fernmeldegeheimnisses. Die Entscheidung, ob der Schutzbereich des Fernmeldegeheimnisses tangiert ist oder nicht, hängt davon ab, ob das Fernmeldegeheimnis die Beteiligten eines Telekommunikationsvorganges weitestgehend so stellt, „wie sie bei einer Kommunikation unter Anwesenden stünden".[29]
Eingriffe in von Art. 10 GG geschützte Bereiche stehen unter Gesetzesvorbehalt.
Als Ermächtigungsgrundlage für die Polizei in Art. 10 GG einzugreifen, kommen die §§ 100a, 100b StPO sowie die §§ 100g-100i StPO in Betracht.
Bei der Telekommunikationsüberwachung kann auch ein Eingriff in das Recht auf informationelle Selbstbestimmung aus Art. 2 I GG in Frage kommen. Dies ist allerdings abhängig von den überwachten Daten.
Dem Bundesnachrichtendienst, dem militärischen Abschirmdienst und dem Verfassungsschutz stehen darüber hinaus noch andere Eingriffsbefugnisse als die der aus dem G 10 - Gesetzt zur Verfügung. Diese stehen der Polizei als Strafverfolgungsbehörde jedoch nicht zur Verfügung. Der Focus dieser Arbeit liegt jedoch nur auf der Betrachtung der Eingriffsmöglichkeiten, die sich für die Polizei aus StPO und TKG ergeben.
Entscheidend für die Bestimmung der einschlägigen Normen ist die Art und Qualität der Daten, die durch die Überwachungsmaßnahmen erhoben werden sollen. Die Vorschriften des TKG und der StPO sind hier in der Begriffsbestimmung identisch. Es lassen sich vier Arten von Daten unterscheiden[30]:

**Bestandsdaten:** Dies sind Daten eines Kommunikationsteilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines

[28] Löffelmann / Walther / Reitzenstein, §3, Rn. 23.
[29] Löffelmann, ZStW 2006, 358; BVerfG, NJW 2006, 976; BVerfG, NJW 2005, 2603.
[30] Siehe zu allem: Löffelmann / Walther / Reitzenstein, §3, Rn. 20.

Vertragsverhältnisses über Telekommunikationsdienste erhoben werden (§ 3 Nr. 3 TKG). Hierzu zählen insbesondere solche Daten, die vom Telekommunikationsdienstanbieter zu Abrechnungszwecken gespeichert werden dürfen (§ 95 TKG), also Name und Anschrift des Teilnehmers sowie die an ihn vergebene Rufnummer.[31]

**Standortdaten:** Hierunter versteht man solche Daten, die in einem Telekommunikationsnetz erhoben oder verwendet werden und die den Standort des Endgerätes eines Benutzers eines Telekommunikationsdienstes für die Öffentlichkeit angeben (§ 3 Nr.19 TKG). Diese Standortdaten sind insbesondere bei der Bestimmung des Standortes eines Mobiltelefons von Bedeutung.[32]

**Verkehrsdaten:** Hierunter werden solche Daten verstanden, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden (§ 3 Nr.30 TKG). Diese Daten wurden in der früheren Terminologie des TKG als „Verbindungsdaten“ bezeichnet, da sie nur im Falle einer Verbindung zwischen zwei Endgeräten anfallen. Zu den Verkehrsdaten zählen unter anderem die Rufnummer und anderweitige Kennungen des Endgerätes sowie der Zeitpunkt des Beginns und die Dauer der Verbindung.[33]

**Inhaltsdaten:** Dieser Begriff wird im Gesetz nicht ausdrücklich definiert. Seine Reichweite ergibt sich in negativer Abgrenzung zu den oben genannten Begriffsbestimmungen. Inhaltsdaten sind danach alle Informationen, die nicht die Umstände der Telekommunikation betreffen, sondern die Kommunikation selbst. Die Inhaltsdaten werden beispielsweise durch das Abhören von Telefongesprächen erhoben.[34]

Die Telekommunikationsüberwachung im Rahmen des strafrechtlichen Ermittlungsverfahrens ist in §§ 100a und 100b StPO geregelt. Um die Normen anwenden zu können müssen die entsprechenden Voraussetzungen gegeben sein.

### 4.1 Materielle Anordnungsvoraussetzungen

Grundsätzlich ist die Überwachung der Telekommunikation nur bei einem qualifizierten Verdacht, der in § 100a II StPO erschöpfend aufgelisteten schweren Straftaten, den sogenannten Katalogstraftaten, zulässig. Der Straftatenkatalog ist recht weit gefächert:

[31] BVerfG, NJW 2010, 833; Meyer-Goßner, § 99, Rn. 16; Hoeren, JZ 2008, 668.
[32] BVerfG, NJW 2007, 351; Hilger, GA 2002, 557; Zöller, GA 2007, 393.
[33] BVerfG, NJW 2009, 2431; Brodowski, JR 2009, 402; Keller, Kriminalistik 2009, 491.
[34] Meyer-Goßner, § 94, Rn. 16a; Hoeren, JZ 2008, 668.

beispielsweise gehören Straftaten gegen die sexuelle Selbstbestimmung (§ 176a ff. StGB); Straftaten gegen das Leben (§ 211 und § 212 StGB), Straftaten gegen das Arzneimittel- und Betäubungsmittelgesetz sowie eine Vielzahl aus weiteren Bereichen dazu.
Bei dem qualifizierten Verdacht genügt es, dass der Verdacht auf einen Versuch einer Anlasstat besteht oder, dass der Versuch einer beliebigen anderen Straftat, durch die eine Anlasstat vorbereitet werden soll, gegeben ist. Ein qualifizierter Verdacht liegt vor, wenn sich ein hinreichend konkreter Anfangsverdacht ergeben hat und durch ausdrücklichen oder schlüssigen Willensakt der Strafverfolgungsorgane das Ermittlungsverfahren betrieben wird. Der Anfangsverdacht muss schon in konkreten Tatsachen bestehen. Für die Beurteilung der Tatsachen, steht ein Spielraum zur Verfügung, in den die kriminalistische Erfahrung und offenkundige Tatsachen des Zeitgeschehens einfließen können.[35]
Ferner muss es sich bei der genannten Anlasstat auch im konkreten Einzelfall um eine Straftat handeln, die gemäß § 100a I Nr.1 und 2 StPO auch im Einzelfall schwer wiegt.[36]
Des Weiteren steht die Zulässigkeit unter dem Vorbehalt einer strengen Subsidiaritätsklausel.[37] Die Subsidiaritätsklausel besagt, dass die Anordnung der Telekommunikationsüberwachung nur in Betracht kommt, wenn die Erkenntnisgewinnung über den Tatvorwurf[38] oder die Ermittlung des Aufenthaltsortes des Beschuldigten durch eine andere weniger belastende Maßnahme aussichtslos oder wesentlich erschwert wäre.[39] Aussichtslosigkeit liegt vor, wenn kein anderes Aufklärungsmittel vorhanden ist. Stehen andere Mittel zur Verfügung, müssen die Erfolgsaussichten abgewogen werden. Eine wesentliche Erschwerung kann angenommen werden, wenn der Einsatz anderer Mittel zu einer erheblichen Verfahrensverzögerung führen würde.[40] Allein ein größerer Arbeitsaufwand rechtfertigt die Maßnahme der Überwachung nur, wenn das Strafverfolgungsinteresse eindeutig überwiegt.[41] Nur nach diesen Abwägungen ist die Maßnahme überhaupt zulässig. Soweit die Voraussetzungen des § 100a I-III StPO erfüllt sind, ist die Maßnahme grundsätzlich zulässig. Sie darf jedoch nur angeordnet werden, wenn zu erwarten ist, dass auch für die Straftat relevante Erkenntnisse gewonnen werden können. Es muss eine Prognose erstellt werden, die ausschließt, dass nur Erkenntnisse aus dem Bereich der privaten Lebensgestaltung gewonnen werden. Diese Prognose muss sich auf tatsächliche Anhaltspunkte stützen.[42]

[35] BGHSt 38, 214; Meyer-Goßner, § 152, Rn.4.
[36] BVerfGE 107, 299; BVerfGE 109, 279; Tetsch, Eingriffsrecht, Kapitel 5.1.2.13.1.2, S.330f..
[37] Meyer-Goßner, § 100a, Rn. 13.
[38] Kinzig, StV 2004, 560; Tetsch, Eingriffsrecht, Kapitel 5.1.2.13.1.2, S.331f..
[39] KK-Nack, §100a, Rn.7.
[40] Meyer-Goßner, § 100a, Rn.9, Rn. 13, 14.
[41] KK-Nack, §100a, Rn. 35; Kinzig, StV 2004, 560.
[42] Meyer-Goßner, § 100a, Rn. 23; Bär, MMR 2008, 215; Rogall, JZ 2008, 818.

## 4.2 Formelle Anordnungsvoraussetzungen

Die Anordnung einer Telekommunikationsüberwachung erfolgt grundsätzlich auf Antrag durch einen Richter nach § 100b I S.1 StPO. Bei dem Vorliegen von Gefahr in Verzuge[43] ist eine Anordnung durch die Staatsanwaltschaft möglich. Zu beachten ist, dass die Ermittlungspersonen nach § 152 GVG eine solche Anordnung nicht treffen können. Erfolgt die Anordnung durch die Staatsanwaltschaft muss sie binnen drei Tagen durch einen Richter bestätigt werden. Bestätigt ein Richter die Anordnung der Staatsanwaltschaft nicht, tritt kein rückwirkendes Außerkrafttreten der Maßnahme ein. Dies hat zur Folge, dass die Erkenntnisse aus diesem Zeitraum verwertet werden können[44] und keinem Verwertungsverbot unterliegen.

Die Anordnung hat prinzipiell schriftlich zu erfolgen und muss erkennen lassen, wer sie erlassen hat. Ferner muss, soweit möglich, der Name und die Anschrift des Betroffen aus ihr hervorgehen.[45] Ferner soll in der Entscheidung die Rufnummer oder eine andere Kennung[46] des Telekommunikationsanschlusses angegeben sein, dies kann eine Kennung des Anschlusses oder des Endgerätes sein.

Ferner muss gemäß § 100b II StPO die Art, Umfang und Dauer der Überwachungsmaßnahme bestimmt sein.[47]

In der zugehörigen Begründung der Überwachungsanordnung sind des weiteren umfänglich die Verdachts- und bisherige Beweislage darzulegen, um die Anordnung der Überprüfung zugänglich zu machen und so dem nachträglichen Rechtsschutz eine Grundlage zu geben.[48]

Eine Anhörung des Betroffenen findet vor Erlass der Anordnung nicht statt. Nach Abschluss der Maßnahme erhält der Betroffene gemäß § 101 StPO eine Benachrichtigung[49] über die durchgeführte Maßnahme mit einem Hinweis auf die Möglichkeit des nachträglichen Rechtschutzes.

## 4.3 Betroffene

§ 100a StPO ermächtigt die Strafverfolgungsbehörden zur Überwachung und Aufzeichnung der Telekommunikation von bestimmten Personen und ermöglicht so einen erheblichen Eingriff in die geschützte Privatsphäre. Die Maßnahme der Überwachung darf sich gemäß § 100a S.2 StPO nur gegen den Beschuldigten oder gegen solche Personen richten,[50] von denen aufgrund bestimmter Tatsachen anzunehmen ist, dass sie Nachrichtenmittler[51] sind

[43] Siehe hierzu: BGH, StV 2008, 63.
[44] Löffelmann / Walther / Reitzenstein, §3, Rn. 26; Knierim, StV 2008, 599.
[45] Meyer-Goßner, §100b, Rn. 3 m.w.N..
[46] BGH, CR 1998, 738; Eckhardt, CR 2007, 336.
[47] Löffelmann / Walther / Reitzenstein, §3, Rn. 26.
[48] Vgl. BGHSt 47, 362 und Fn. 33.
[49] Meyer-Goßner, § 101, Rn. 5, 6; Puschke / Singelnstein, NJW 2008, 113.
[50] SK-Rudolphi, §100a, Rn 16.
[51] Siehe hierzu: Beulke, §12 Rn. 253; Tetsch, Eingriffsrecht, Kapitel 5.1.2.13.1.2, S.331f..

oder dass gemäß § 100a S.3 StPO der Beschuldigte ihren Anschluss benutzt.[52] Zu beachten ist die ausgeübte Tätigkeit von Berufsgeheimnisträgern im Sinne des §§ 160a, 53 StPO, wie zum Beispiel Ärzten, Rechtsanwälten und Geistlichen. Dies ist im Rahmen der Verhältnismäßigkeitsprüfung zu berücksichtigen. So dürfen zum Beispiel mandatsbezogen Gespräche zwischen Verteidiger und Beschuldigtem nicht abgehört werden, da andernfalls § 148 StPO ins Leere liefe.[53]

### 4.4 Mitwirkungspflicht der Telekommunikationsanbieter

Durch § 100b III StPO ist die Mitwirkungspflicht der verschiedenen Telekommunikationsanbieter bei der Durchführung einer Überwachungsmaßnahme geregelt. Einzelheiten in Bezug auf die Durchführung und die zu erbringenden Leistungen der Telekommunikationsanbieter sind in dem TKG und der TKÜV festgelegt. Insbesondere sind eine Ausleitung einer Kopie der digitalisierten Telekommunikationssignale an die Strafverfolgungsbehörden zu ermöglichen und unverzüglich die erforderlichen Auskünfte zu erteilen.[54] Anderen Personen darf der verpflichtete Anbieter keine Angaben machen. Das Mithören und die Kenntnisnahme vom Inhalt der Mitteilung sind auf den Richter, die Staatsanwaltschaft und ihre Ermittlungspersonen begrenzt.[55]
Hingegen ist der Telekommunikationsanbieter nicht verpflichtet, auf eigene Kosten technische Einrichtungen vorzuhalten und entsprechende organisatorische Vorkehrungen zu treffen.[56] Entstandene Kosten sind den Verpflichteten zu erstatten.[57]
Gleiches gilt auch für Anbieter, die nur Telekommunikationsdienste innerhalb eines geschlossenen Systems zur Verfügung stellen,[58] zum Beispiel Intranet oder ausschließlich zum Eigenbedarf in einem Unternehmen betriebenen Kommunikationsanlagen.

### 4.5 Beendigung der Maßnahme / Befristung

Gemäß § 100b IV StPO ist die Überwachungsmaßnahme grundsätzlich ohne vermeidbare Verzögerungen zu beenden, sobald die Voraussetzungen für die Anordnung nicht mehr vorliegen. Das Fortbestehen der Anordnungsvoraussetzungen gemäß § 100a StPO unterliegt der ständigen Überprüfung. Die endgültige Entscheidung über die Beendigung der Überwachung trifft in der Regel die Staatsanwaltschaft.

---

[52] Zu allem Löffelmann / Walther / Reitzenstein, §3, Rn. 25.
[53] Beulke / Ruhmannseder, Rn. 513; BVerfG, NJW 2007, 2749; Beulke, §12, Rn. 254; Beulke / Ruhmannseder, StV 2011, 180; StV 2011, 252.
[54] Meyer-Goßner, § 100b, Rn.7, 8.
[55] Joecks, JA 1983, 60.
[56] Vassilaki, JR 2000, 446; BVerfG, NJW 2010, 833; Eckhardt, CR 2007, 336.
[57] Meyer-Goßner, § 100b, Rn.13.
[58] Meyer-Goßner, § 100b, Rn. 8 m.w.N..

Nach § 100b II StPO ist die Überwachungsmaßnahme auf höchstens drei Monaten zu befristen. Die Maßnahme kann gegebenenfalls mehrfach um jeweils drei Monate verlängert werden[59], wenn die Anordnungsvoraussetzungen weiterhin vorliegen.
Nach der Beendigung sind das zuständige Gericht und der verpflichtete Telekommunikationsdienstanbieter zu informieren.[60] Ferner besteht eine Benachrichtigungspflicht der Staatsanwaltschaft gegenüber dem Betroffenen. Hierbei ist es gleichgültig, ob die Telekommunikationsüberwachung zu einem Erfolg geführt hat oder nicht. Auch ist es irrelevant, ob die gewonnen Erkenntnisse verwertet werden.[61] Die Benachrichtigungspflicht dient allein der Gewährleistung eines effektiven Rechtsschutzes des betroffenen Grundrechtes. Auf diesem Weg erhält der Betroffene im Sinne des Art. 103 I GG nachträglich rechtliches Gehör.[62]
Die Resultate der Ermittlungsmaßnahme sind nach der Beendigung dem Gericht darzulegen.

### 4.6 Verwendung erlangter Daten / Erkenntnissen

Die personenbezogenen Daten, die durch eine Überwachungsmaßnahme nach § 100a StPO erlangt wurden, können gemäß auch in anderen Strafverfahren verwendet werden.[63]
Die Grundlage für die Regelung nach § 100a StPO bildet der hypothetische Ersatzeingriff[64] und der datenschutzrechtliche Zweckbindungsgrundsatz. Dementsprechend sind die erlangten Daten prinzipiell nur für den einen bestimmten Zweck der Anordnung zu verwenden, für den sie erhoben wurden. Diese Ausnahme soll dann gelten, wenn die Daten für den anderen Zweck rechtmäßig hätten erhoben werden dürfen.[65]
Das Überwachen einer Telekommunikationsverbindung ist, wie bereits dargestellt, nur bei Verdacht auf eine Katalogstraftat gemäß § 100a StPO zulässig. Bei einer Überwachung greifen die Strafverfolgungsbehörden mitunter sehr weit in die Grundrechtssphäre der Betroffenen ein. Daher sind bei einigen Eingriffen sehr hohe Schwellen gesetzt. Eine Grundlage unseres Rechtssystems ist die Annahme, dass Hoheitsträger die ihnen durch Gesetzt und Verordnungen gesetzten Eingriffsgrenzen achten und respektieren. Wenn dies nun im konkreten Eingriff einmal nicht der Fall ist und Beweismittel rechtswidrig erlangt werden, stellt sich die Frage, ob die Beweise verwertet werden dürfen oder nicht. Dies kann im Einzelfall bedeuten, dass der Straftatvorwurf nicht mehr bewiesen werden kann.
Um diese offene Problematik zu lösen, gibt es den hypothetischen Ersatzeingriff. Es wird geprüft, ob die erlangten Erkenntnisse durch eine andere Maßnahme rechtmäßig erlangt

[59] Löffelmann / Walther / Reitzenstein, §3, Rn. 26.
[60] Löwe-Rosenberg / Schäfer, StPO, §100b, Rn. 33.
[61] Meyer-Goßner, § 101, Rn.15; BGH 36, 305.
[62] BVerfG, NJW 2010, 833; BGH 36, 305.
[63] Meyer-Goßner, § 100a, Rn. 32, 33.
[64] Beulke, § 12, Rn. 233a.
[65] Löffelmann / Walther / Reitzenstein, §3, Rn. 29; Meyer-Goßner, §100a, Rn.32f..

hätten werden können.[66] Auf diese Weise kann durch die Anwendung des hypothetischen Ersatzeingriffs ein unrechtmäßiger Eingriff legitimiert werden. Die Anwendung des Ersatzeingriffs ist nicht unproblematisch, da die hypothetische Annahme nicht eine sorgfältige ex-ante Prüfung[67] verdrängen darf. Der BGH bejaht die Anwendung für die Telekommunikationsüberwachung weitestgehend, sofern die Strafverfolgungsbehörden nicht willkürlich gehandelt haben.[68] Zu den Beweiserhebungsverboten und den Verwertungsverboten später mehr.
Demnach können diese Daten nur ausnahmsweise auch für andere Zwecke verwendet werden, wenn sie hierfür rechtmäßig hätten erhoben werden dürfen. Allerdings nur für den Zweck in Form eines anderen Strafverfahrens und hier zu Beweiszwecken. Eine Verwendung in weiteren Verfahren als Ermittlungsansatz ist allerdings uneingeschränkt zulässig. Mit anderen Strafverfahren sind solche gemeint, die nicht mit der zugrundeliegenden Anlasstat der Überwachungsanordnung in einem engen inneren Zusammenhang stehen.[69]
Nach Abschluss des Verfahrens sind die erlangten personenbezogenen Daten gemäß § 100a IV StPO aus dem Verfahren unter Aufsicht der Staatsanwaltschaft zu vernichten, sofern sie nicht mehr für die Strafverfolgung erforderlich sind. Die Vernichtung der Daten ist zu dokumentieren.[70]

### 4.7 Rechtschutz

§ 101 StPO regelt die grundrechtssichernde Verfahrensregelung für verdeckte Ermittlungsmaßnahmen. Zunächst muss der Betroffene der verdeckten Maßnahme benachrichtigt werden. Die Benachrichtigung erfolgt erst, wenn dieses ohne Gefährdung des Untersuchungszweck, des Lebens, der körperlichen Unversehrtheit und der persönlichen Freiheit einer Person und von bedeutenden Vermögenswerten und gegebenenfalls der Verwendung eines verdeckten Ermittlers möglich ist.[71] Eine Gefährdung des Untersuchungserfolgs kommt so lange in Betracht, wie erwartet werden kann, dass mit der Hilfe der in § 101 I StPO genannten Maßnahmen Beweismittel aufgefunden oder beweiserhebliche Mitteilungen aufgefangen werden können. Das wird in der Regel solange der Fall sein, wie das Verfahren noch nicht offen geführt wird. Daher kann wohl angenommen werden, dass eine Gefährdung solange anzunehmen ist, wie das Verfahren durch die Staatsanwaltschaft noch nicht gemäß § 169a StPO förmlich abgeschlossen ist.[72]

[66] Mosbacher, JuS 2008, 125; BGH 31, 304.
[67] Siehe hierzu: Beulke, § 23, Rn. 475; Rn. 233a; Rn 483.
[68] Beulke, § 12, Rn.233a-233d; BGH, NStZ 1989, 375; Kinzig, StV 2004, 560.
[69] Küpper, JZ 1990, 416.
[70] Siehe zu allem: Löffelmann / Walther / Reitzenstein, §3, Rn. 26 m.w.N..
[71] Henrichs, Kriminalistik 2008, 169.
[72] Zu allem: Burghardt, HRRS 2009, 567; Meyer-Goßner, §101, Rn. 15, 25.

Bei Maßnahmen nach § 100a StPO und § 100g StPO sind alle Beteiligten, in deren Grundrechte eingegriffen wurde, zu benachrichtigen, nicht nur der Beschuldigte einer Straftat. Personen die nur vorübergehend bzw. nur geringfügig von der Maßnahme betroffen waren, sind von der Benachrichtigung auszuklammern; es darf sich allerdings nicht um einen erheblichen Grundrechtseingriff im Einzelfall handeln.[73] In Ausnahmefällen kann die Staatsanwaltschaft mit Zustimmung des Gerichts von einer Benachrichtigung absehen.[74] Die Voraussetzung für die Zurückstellung der Benachrichtigung liegen in der Regel vor, wenn mit einer Gefährdung des Lebens, der Unversehrtheit und der persönlichen Freiheit einer Person, zum Beispiel einem verdeckten Ermittler, zu rechnen ist. Als weiterer Grund kommt in Betracht, dass weitere Ermittlungen gegen andere Personen wesentlich erschwert oder gar vereitelt würden, wenn eine Benachrichtigung erfolgt.
Die Benachrichtigungspflicht obliegt der Staatsanwaltschaft. Für diese Benachrichtigung ist eine förmliche Zustellung nicht zwingend erforderlich. Der Betroffene ist auf den nachträglichen Rechtsschutz hinzuweisen. Desweiteren ist dem Betroffenen Einblick in den Umfang der durchgeführten Maßnahme zu gewähren. Nicht entscheidend ist, ob die erlangten Erkenntnisse und Daten verwertet worden sind oder nicht. Auch ist es nicht ausschlaggebend, ob die Maßnahme erfolgreich war.[75]
Die Benachrichtigungspflicht dient der Gewährleistung eines effektiven Schutzes der jeweils betroffenen Grundrechte.[76]
Der Betroffene kann sich gegen die heimliche Ermittlungsmaßnahme in der Form wenden, dass er einen Antrag auf Überprüfung der Rechtmäßigkeit stellt. Die Überprüfung beinhaltet auch eine Kontrolle der Art und Weise der Maßnahme.[77]
Dem Betroffenen wird auf diesem Weg nachträglich rechtliches Gehör im Sinne des Art 103 I GG gewährt und er erhält die Möglichkeit sich gegen die Eingriffsmaßnahme zur Wehr zu setzen.

## 5 Erhebung von Telekommunikationsdaten

Der Anwendungsbereich von § 100a StPO ist vielfältig und erstreckt sich nicht nur auf die alltägliche Form des Telefonierens und Fernschreibens. Vielmehr ist nahezu jede Art der Nachrichtenübermittlung umfasst. Fraglich ist, unter welchen Voraussetzungen auf die einzelnen Daten zugegriffen werden kann.

[73] Meyer-Goßner, §101, Rn.11f..
[74] Vertiefend hierzu: Puschke / Singelnstein, NJW 2008, 113.
[75] BGH 36, 305; Meyer-Goßner, § 101, Rn.15.
[76] Meyer-Goßner, § 101, Rn.25 m.w.N..
[77] Siehe hierzu vertiefend: Burghardt, HHRS 2009, 567; Singelnstein NStZ 2009, 481.

## 5.1 Überwachung von E-Mails

Beim Zugriff auf E-Mails ist für die Ermächtigungsgrundlage wie folgt zu differenzieren: Der Austausch von E-Mails erfolgt unter Einschaltung von Servern der Provider. Auf diesen werden die Mails zwischengelagert, bis sie vom Empfänger abgerufen werden. Fraglich ist, unter welchen Voraussetzungen ein Zugriff auf die Daten stattfinden darf. Für die rechtliche Einordnung der Überwachung von E-Mails sind 3-Phasen[78] zu unterscheiden:

*Phase 1: Übermittlungsvorgang vom Absender zum Server des Provider*
*Phase 2: die Nachricht „ruht" auf dem Server des Providers*
*Phase 3: der Empfänger ruft die Nachricht vom Server ab*

Während des Übermittlungsvorgangs vom Absender zum Server und vom Server zum Empfänger gelten unstreitig die hohen Eingriffsvoraussetzungen des § 100a StPO, da in diesen Fällen, eindeutig eine Kommunikation stattfindet.
Problematisch ist der Zugriff auf die Mails während der Zwischenspeicherung auf dem Mailserver des Providers. BGH und BVerfG bewerten die kurzzeitige Zwischenspeicherung beim Provider rechtlich als Unterbrechung des Kommunikationsvorganges[79] und verneinen daher die Anwendbarkeit des Art. 10 GG. Daraus folgt, dass mangels eines Telekommunikationsvorganges die Eingriffsvoraussetzungen der Sicherstellung und Beschlagnahme im Sinne der § 94ff. StPO analog für den Zugriff auf Daten, die beim Provider gespeichert sind, ausreichen. Die Rechtsprechung begründet dies damit, dass die besondere Schutzbedürftigkeit von Grundrechtsträgern im Bereich des Art. 10 GG durch die mangelnde Beherrschbarkeit von E-Mail - Übermittlungen aufgrund der Nutzung von Diensten eines Dritten, den Providern, bei dem Telekommunikationsvorgang nicht gegeben ist.
Der Auffassung, dass der Kommunikationsvorgang in seine rein technischen Gesichtspunkte aufgespalten und unterschiedlich bewertet wird, kann nach Ansicht des Verfassers nicht gefolgt werden. Für den Nutzer stellt sich der für ihn nachvollziehbare Übermittlungsvorgang als ein einheitliches Geschehen dar, insofern vertraut er auf den Schutz des Fernmeldegeheimnisses im Sinne des Art. 10 GG.[80]
Das BVerfG unterstellt zwar die E-Mail - Übermittlung dem Schutz von Art. 10 GG, da dem Fernmeldegeheimnis bei einer umfassenden Einzelfallprüfung in der Verhältnismäßigkeit genüge getan sei und wendet die Eingriffsvoraussetzung des §§ 94 ff. StPO i.V.m. der Postbeschlagnahme für den Zugriff auf E-Mails, die beim Provider lagern, an.

[78] KK-Knack, § 100a, Rn. 7ff.; Palm / Roy, NJW 1996, 1791; andere Phasen-Modelle bei: Brodowski, JR 2009, 402 (7 Phasen); Beulke, § 12, Rn. 253b (4 Phasen).
[79] BGH, NStZ 2009, 397; BVerfG, StV 2009, 617.
[80] Vgl. hierzu Löffelmann / Walther / Reitzenstein, § 3, Rn. 30.

Die Lösung über die Sicherstellung und Beschlagnahme[81] birgt allerdings die Gefahr, dass das Schutzniveau für die E-Mail - Kommunikation insgesamt abgesenkt wird, da in eine für diese Kommunikation typische technische Phase unter erleichterten Eingriffsvoraussetzungen eingegriffen werden kann.[82]
Hat der Empfänger die Daten empfangen, bestehen nicht mehr die spezifischen Gefahren einer räumlich distanzierten Kommunikation und der Empfänger kann frei darüber entscheiden, ob und wie er den Kommunikationsinhalt speichert und archiviert. Daher liegt hier nicht mehr ein von Art. 10 GG geschützter Bereich vor und auf die Daten kann unter den Voraussetzungen des §§ 94 ff. StPO zugegriffen werden.

### 5.2 Abhören von Mailboxen

Es ist fraglich, ob §§ 100a, b StPO bezüglich der Überwachung von Mailboxen anwendbar ist. Hierbei ist zwischen zwei Konstellationen zu differenzieren.
Die Überwachung von Datenübermittlungen von oder zu einer angeschlossenen Mailbox ist erfasst, da es sich dabei um Telekommunikation im Sinne von § 100a StPO handelt. Nach der herrschenden Meinung ist jegliche Nachrichtenübermittlung, nicht nur die herkömmliche Form des Telefonierens erfasst.[83]
Anders gelagert ist der Zugriff auf Informationen, die in einer Mailbox abgespeichert sind. Es liegt hier eine Datendeponierung und nicht eine Übermittlung vor. Es stellt sich nun die Frage, ob auf deponierte Beweismittel die Beschlagnahmevorschriften nach §§ 94 ff. StPO und §§ 102 ff. StPO oder doch noch § 100a StPO an wenden ist. Eine unmittelbare Anwendung der Sicherstellungs- und Beschlagnahmenormen scheidet aus, da es sich nicht um körperliche Gegenstände und nicht um ein körperliches Eindringen in Räume handelt. Möglich wäre aber eine analoge Anwendung der §§ 94, 102 StPO. Eine analoge Anwendung ist eröffnet,[84] da es Parallelen zur Durchsuchung gibt. Es wird von außen auf ein Gerät zugegriffen, das in dem von Art. 13 GG geschützten Bereich installiert worden ist.[85]
BVerfG und BGH legen § 100a StPO im Sinne des technischen Fortschritts weit aus[86] und fassen daher die Abfrage einer Mailbox noch in den Anwendungsbereich der Telefonüberwachung. Der Eingriff erfolgt zwar von außen, allerdings rein über das von außen zugängliche Leitungsnetz. Daher wird der technische Komplex der Fernmeldeeinrichtung nicht verlassen und zur Durchführung der Überwachungsmaßnahme die Wohnung nicht betreten. Daher wird nicht in den Kernbereich des Art. 13 GG eingegriffen. Aufgrund der Parallelen zur Durchsuchung wendet die Rechtsprechung die §§

[81] Beschlagnahme gem. §§94 ff. StPO analog.
[82] Siehe Beulke, § 12, Rn. 253b; Roxin / Schünemann, § 26, Rn.4; Beulke / Ruhmannseder, Rn. 507f..
[83] KK-Nack, § 100a, Rn. 2.
[84] Larenz / Canaris, Methodenlehre, S. 202.
[85] BGH, NStZ 1997, 247; Vassilaki, JR 2000, 447.
[86] Palm / Roy, NJW 1997, 1904; Kudlich, JuS 1998, 209.

102 ff. StPO sinngemäß an und es kommt zu zwei Einschränkungen: Sofern die Überwachung sich gegen einen Unverdächtigen richtet, darf nur nach bestimmten, das heißt konkreten Beweismitteln gesucht werden. Folglich nur nach Daten, die für eine konkrete Straftat von Belang sind. Die zweite Einschränkung wird aus § 105 StPO abgeleitet. Die Maßnahme mit dem Eingriff muss für einen Richter kontrollierbar bleiben. Daraus ergibt sich, dass ein mehrfaches Überwachen der Mailbox nicht gestattet ist. Der Zugriff auf die Mailboxdaten darf nur einmal erfolgen.[87]

Diese Auffassung der Rechtsprechung wird von der Literatur[88] in Frage gestellt. Da schon begrifflich keine Überwachung der Telekommunikation vorliege, sondern ein aluid.[89] Hier würde nicht ein Ermittlungsbeamter als Dritter die Kommunikation zwischen zwei Personen überwachen, sondern der Beamte würde von sich eine Verbindung herstellen und sich einwählen. Daher könne hier nicht von Überwachen gesprochen werden. Für diesen heimlichen Zugriff auf Mailboxdaten prangert die Literatur an, gebe es keine Ermächtigungsgrundlage.

Die Literatur vernachlässigt im Hinblick auf die Entscheidung des BVerfG[90], dass im Rahmen des technischen Fortschritts der § 100a StPO weit auszulegen ist. Ferner findet die Tatsache, dass die in einer Mailbox gespeicherten Informationen auch das Merkmal der Telekommunikation erfüllen, keine Berücksichtigung. Besonderheit, bei der Nutzung eines Mailboxsystems ist, dass die Nachrichtenübermittlung noch nicht beendet ist, da der Empfänger den Kommunikationsinhalt noch nicht zur Kenntnis nehmen konnte. Daher ist der Rechtssprechungsmeinung zu folgen und im Ergebnis ist logischerweise § 100a StPO anwendbar für die Abfrage von Daten von einer Mailbox.

Hingegen ist § 100a StPO nicht mehr anwendbar, wenn ein Telefongespräch bereits endgültig beendet ist und die Daten nur noch im Empfangsgerät gespeichert sind.[91] Der Schutzbereich des Art. 10 GG endet, wenn die Nachricht den Empfänger erreicht hat und der Übertragungsvorgang beendet ist. Die Daten werden folglich nicht mehr durch Art. 10 GG geschützt, sondern durch das Recht auf informationelle Selbstbestimmung aus Art. 2 I i.V.m. Art. 1 I GG.[92] Soll nun auf diese Daten zurückgegriffen werden, müssen nicht die Schutzvorschriften über die Telekommunikationsverbindungen beachtet werden, sondern die Vorschriften der Sicherstellung und Beschlagnahme.[93]

Festzuhalten bleibt, dass solange der Kommunikationsvorgang noch nicht vollständig beendet ist, ist § 100a StPO einschlägig ist. Sofern die Kommunikation abgeschlossen ist

[87] Siehe hierzu: Kudlich, JuS 1998, 209; BGH, NStZ 1997, 247.
[88] Palm / Roy, NJW 1997, 1904.
[89] Bär, CR 1996,675; 1996, 744; Sankol, JuS 2006, 698.
[90] BVerfG, NJW 1978, 313.
[91] Vgl. BVerfGE 115, 166.
[92] Götz, Kriminalistik 2005, 300; Thiede, Kriminalistik 2005, 346; Jahn, JuS 2006, 491.
[93] Vgl. Beulke, § 12, Rn.254b, 253a; Schlegel, HRRS 2007, 44.

muss der Zugriff auf die Daten nach den Regeln der Sicherstellung und Beschlagnahme erfolgen.

### 5.3 Überwachen von Mobiltelefonen im Stand - by - Modus

Die Daten, die aus einem Zugriff auf Standortdaten stammen, können für die Strafverfolgungsbehörden bedeutsam sein, um ein Alibi eines Beschuldigten nachvollziehen zu können oder um Bewegungsbilder zu erstellen. In jüngster Vergangenheit haben sie deutlich an Bedeutung für die Praxis gewonnen.[94]

Ist ein Mobiltelefon eingeschaltet, wird aber nicht genutzt, erzeugt es in regelmäßigen Abständen einen Funkimpuls, mit dem sich das Handy in einer Funkzelle anmeldet. Auf diese Weise bleibt die Empfangsbereitschaft erhalten. Bei diesem Funkimpuls handelt es sich um Standortdaten, bei denen die Gerätenummer, die Kartennummer und die Daten, in welcher Funkzelle das Mobiltelefon sich wann eingewählt hat, mit übermittelt werden. In der Regel archiviert der Telekommunikationsanbieter diese Daten allerdings nicht.

Fraglich ist, unter welchen Eingriffsvoraussetzungen auf diese Daten zugegriffen werden kann. Da die Daten, die im Stand-by Modus erzeugt werden nicht an einen Empfänger gerichtet sind, können sie somit auch keinen Kommunikationsvorgang darstellen. Daher stellt sich die Frage, ob hier überhaupt der Schutzbereich des Fernmeldegeheimnisses eröffnet ist oder ob die Daten eher dem Recht auf informationelle Selbstbestimmung unterfallen. Bei den Standortdaten handelt es sich nicht um Daten einer Kommunikation, daher ist der Schutzbereich der informationellen Selbstbestimmung eröffnet und nicht der des Fernmeldegeheimnisses.[95] Und in diesen kann auf Grundlage der §§ 94, 98 StPO eingegriffen werden.

Eine Verpflichtung des Telekommunikationsanbieters zur Mitwirkung bzw. zur Mitteilung nicht gespeicherter Standortdaten gibt es nicht. Sollten sie aber dennoch nachvollziehbar sein, ist er nach § 7 I TKÜV befugt, die Daten weiterzuleiten.

Die Gewinnung der Daten in Echtzeit kann mittels eines IMSI- / IMEI- Catchers erfolgen. Hierzu später mehr unter 4.7. Oder aber die Verkehrsdaten können nach § 100g I StPO mittels eines Phonetracker[96] erhoben werden.

Zu untersuchen ist ferner noch, ob es möglich ist, den Telekommunikationsanbieter zu verpflichten, zukünftig anfallende Standortdaten zu speichern und auszuhändigen. Standortdaten fallen unter die Legaldefinition des § 3 Nr. 22, 23 TKG. Insofern ist es möglich, mit einer entsprechenden Anordnung nach §§ 100a, 100b StPO den

[94] Beachte hierzu: Henrichs, Kriminalistik 2008, 169.
[95] Keller, TKÜ, S. 31; Zöller, GA 2007, 393; Hilger, GA 2002, 557.
[96] Welp, GA 2002, 535; Korn, HRRS 2009, 112; Hoeren, JZ 2008, 668.

Telekommunikationsanbieter zu verpflichten, die anfallenden Standortdaten zu speichern und zu übergeben.[97]

### 5.4 Überwachen von Raumgesprächen

Ein weiterer konfliktträchtiger Bereich ist die Frage, welche Vorschrift Anwendung findet, wenn ein Gespräch über eine Telekommunikationsverbindung übertragen wird, die Verbindung aber nicht willentlich zustande gekommen ist. Es geht also um die Konstellation, dass zum Beispiel ein Mobiltelefon wie eine Abhöreinrichtung genutzt wird. Fraglich ist, ob auch hier §§ 100a, 100b StPO anwendbar sind oder ob der richtige Bezugspunkt § 100f StPO beziehungsweise, falls die Gespräche in der Wohnung stattfinden, § 100c StPO ist.[98] Der BGH[99] hat in einem solchen Sachverhalt den subjektiven Willen des Betroffenen vernachlässigt und darauf abgestellt, dass der Betroffene objektiv bereit war mittels seines Mobiltelefons zu kommunizieren. Das Gericht wendet hier nicht den rein technischen Begriff der Telekommunikation gemäß §§ 100a, 100b[100] StPO an, sondern legt den Schwerpunkt auf den Kommunikationsinhalt, der durch Art. 10 GG geschützt ist.
§ 100c StPO und § 100f StPO sind von den Eingriffsvoraussetzungen beide mit den Anordnungsvoraussetzungen des § 100a StPO vergleichbar[101]. Obendrein findet ein Kommunikationsvorgang statt, der zwar ungewollt ist, aber dennoch in den Schutzbereich von Art. 10 GG fällt. Die Anwendung von § 100a I StPO ist praxisnäher und im Rahmen der grundrechtssichernden Regelung des § 101 StPO in Hinsicht auf etwaige Verwertungsverbote und den Rechtschutz zu würdigen.[102]

### 5.5 Einsatz IMSI- / IMEI-Catchers / Lokalisierung eines Mobiltelefons

Der Einsatz eines IMSI- / IMEI- Catchers richtet sich nach § 100i StPO. Durch den Einsatz des Gerätes wird das Auslesen der Kartennummer IMSI und oder der Gerätenummer IMEI eines auf Stand-by geschalteten Mobiltelefons ermöglicht, ferner ist eine Standortbestimmung des Gerätes möglich.
Bei der IMSI handelt es sich um eine einmalig vergebene Kennnummer, die eine feste Zuordnung eines jeden Vertragspartners eines Mobilfunkanbieters darstellt. Sie ist auf der SIM-Karte gespeichert, welche jedem Teilnehmer mit Abschluss eines Mobilfunkvertrages ausgehändigt wird. Aufgrund der Einmaligkeit ist es möglich, einen Mobilfunkteilnehmer weltweit zu identifizieren. Sie besteht aus einer fünfzehnstelligen Zahlenfolge, von denen die ersten fünf Ziffern das Land und den Netzbetreiber erkennen lassen. Anhand der folgenden

[97] BGH, NJW 1997, 1934; BGH, NJW 2001, 1587.
[98] KK-Nack, § 100a, Rn.40; BGHSt 31, 296; Löffelmann / Walther /Reitzenstein, § 3, Rn. 33f..
[99] BGH, NJW 2003, 2034.
[100] Legaldefinition siehe § 22 Nr.3 TKG.
[101] BGH 53, 294; BGH 34, 39.
[102] BGH, StV 1997, 400; KK-Kuckein, § 337, Rn.30; a.A. Braum, JZ 2004, 128.

Ziffern können die Netzbetreiber die gespeicherten Bestandsdaten des Teilnehmers ermitteln.[103]

Bei der IMEI handelt es sich ebenfalls um eine weltweit einmal vergebene Kennnummer, welche mit jedem Mobilfunkgerät elektronisch verbunden ist.

Jedes Mobilfunknetz ist in Funkzellen unterteilt, mit denen eine bestimmte geographische Fläche abgedeckt wird. Die Größe der Funkzellen variiert. Die Funkzellen können ausgehend von der Mitte, dem Sendemasten, wenige hundert Meter groß sein oder bis hin zu mehreren Kilometern.[104]

Die Karten- und die Gerätenummer haben im Bereich der mobilen Telekommunikation eine enorme Bedeutung. Generell lockt sich jedes eingeschaltete Handy bei der Basisstation derjenigen Funkzelle an, in deren Reichweite es sich gerade befindet. Bei diesem Vorgang werden die beiden Kennungen mittels Funksignal vom Handy an den Netzbetreiber übermittelt und von diesem gespeichert. Durch dieses sich permanent wiederholende Einloggen ist die durchgehende Erreichbarkeit des Endgerätes sichergestellt.[105]

Die Vorschrift des §100i StPO ermöglicht zwei Eingriffsvarianten. Bei der einen handelt es sich um die Lokalisierung des genauen Standortes eines Mobiltelefons, um eine Person, die einer Straftat von erheblicher Bedeutung beschuldigt ist, festzunehmen.[106] Hierzu simuliert das Gerät eine Funkzelle. Dies wird von unterschiedlichen Standorten wiederholt. Dadurch, dass sich das Mobiltelefon wiederholt in die simulierte Funkzelle einwählt, kann der Standort des Endgerätes ermittelt werden.

Die Lokalisierung mit einem IMSI-Catcher ist gemäß § 100i I Nr. 2 StPO möglich und zulässig.[107]

Bei der Regelung nach § 100i I Nr. 1 StPO handelt es sich um eine Maßnahme, die darauf abzielt, eine Telekommunikationsüberwachung vorzubereiten. Sind die IMSI- / IMEI-Kennung bekannt, kann die zugehörige Rufnummer bei dem Mobilfunkanbieter ermittelt werden und die mit dem Handy geführte Telekommunikation überwacht werden.[108] Der Einsatz des IMSI- / IMEI- Catchers ist in der Regel mit Observierungsmaßnahmen kombiniert.

Nach dem BVerfG fällt der Einsatz des IMSI- / IMEI- Catchers nicht in den Schutzbereich von Art. 10 GG,[109] sondern tangiert nur das Recht auf informationelle Selbstbestimmung und das Recht der allgemeinen Handlungsfreiheit.[110] Im Falle der Vorbereitung einer Telekommunikationsüberwachung ist die Maßnahme nur unter den Voraussetzungen des §

---

[103] Harnisch / Pohlmann, HRRS 2009, 202; Hilger, GA 2002, 557; Keller TKÜ S.40.
[104] Artkämper, Kriminalistik 1998, 202; Harnisch / Pohlmann, HRRS 2009, 202.
[105] Keller, TKÜ, S. 42; KK-Nack, § 100a, Rn.11; §100i Rn.5.
[106] BVerfG, NJW 2007, 351; Hilger, GA 2002, 557; KK-Senge, §81g, Rn. 2; Beulke, § 2 Rn. 130f..
[107] Harnisch / Pohlmann, HRRS 2009, 202; KK-Nack, § 100i, Rn.4; Meyer-Goßner, §100i, Rn.10; Keller, TKÜ, S.30.
[108] Löwe-Rosenberg / Schäfer, StPO, § 100i, Rn.3.
[109] BVerfG, NJW 2007, 351; Meyer-Goßner, § 100i, Rn. 1; Korn, HRRS 2009, 113.
[110] Heintschel-Heinegg, JA 2007, 75; Beulke, § 12, Rn. 254c.

100a StPO zulässig. Die Anordnung muss gemäß § 100i IV i.V.m. § 100b II StPO schriftlich ergehen und ist auf höchstens sechs Monate zu befristen, eine mehrfache Verlängerung ist möglich. Sollten funktionsbedingt personenbezogene Daten Dritter festgestellt werden, sind diese unverzüglich zu löschen. [111]

Neuere Geräte können auch die Kommunikation des gesuchten Mobiltelefons überwachen. Soweit der IMSI- Catcher das Mithören laufender Gespräche in Echtzeit ermöglicht,[112] ist die Nutzung nicht durch § 100i StPO gedeckt und bedarf der zusätzlichen Anordnung nach §§ 100a, 100b StPO.

Der Einsatz des IMSI- / IMEI-Catchers im Rahmen der Strafverfolgung ist unter den Voraussetzungen des § 100i StPO zulässig.

### 5.6 Einsatz MAC-Catcher

Der MAC-Catcher ist das Pendant zum IMSI- / IMEI-Catcher. Mit ihm kann man die hardwarespezifische einmalige Kennung eines in ein W-LAN eingebunden Gerätes ermitteln. Die Ermittlung der Kennung dient der Vorbereitung einer Überwachung der Telekommunikation gemäß § 100a StPO. Hat man die Kennung und ist die Überwachung aufgeschaltet, kann man die Daten die mittels W-LAN übermittelt werden abfangen und auswerten. In Betracht kommen hier vor allem E-Mails, Chat oder Downloads.

Wie auch beim IMSI-Catcher stellt sich die Frage nach einem Eingriff in grundrechtlich geschützte Bereiche. Zunächst wäre an das Recht auf Unverletzlichkeit der Wohnung gemäß Art. 13 I GG zu denken. Eingriffe bestünden in Form eines körperlichen Betretens oder eines technischen Spähangriffes. Besonderheit beim W-LAN ist, dass der Betreiber bei einer offenen Nutzung des W-LAN eine Ausstrahlung der Funkwellen in den öffentlichen Raum in Kauf nimmt, daraus resultiert nach dem BVerfG ein geringerer Schutzanspruch.[113] Er entlässt die Räumlichkeit in gewissem Umfang aus der privaten Intimsphäre.[114] Werden nun diese nach außendringenden Daten aufgefangen, liegt kein Eingriff in den Schutzbereich aus Art. 13 GG vor.

Ferner könnte Art. 10 GG betroffen sein. Hierbei ist zu unterscheiden zwischen Stand-by Modus und aktiver Nutzung. Bei aktiver Nutzung der Netzwerkverbindung liegt unzweifelhaft Kommunikation vor, da Daten menschlich veranlasst empfangen und gesendet werden. Somit ist das Fernmeldegeheimnis betroffen und es bedarf einer Anordnung nach § 100a StPO.

[111] Thiede, Kriminalistik 2003, 165; Löffelmann / Walther / Reitzenstein, § 3, Rn. 46-48.
[112] Siehe hierzu Harnisch / Pohlmann, HRRS 2009, 204.
[113] Siehe: BVerfG 32, 54.
[114] Ruthig, JuS 1998, 506; Jarass / Pieroth, Art. 10, Rn. 5.

Im Stand-by Modus werden zwar auch Daten gesendet und empfangen. Dieser Austausch ist allerdings nicht menschlich veranlasst. Es liegt folglich keine Kommunikation im Sinne des Fernmeldegeheimnisses vor, in Art. 10 GG wird nicht eingegriffen.[115]
Des Weiteren könnte das Recht auf informationelle Selbstbestimmung betroffen sein. Hierzu müsste man über die MAC-Kennung Rückschlüsse auf den Besitzer ziehen können. Die MAC-Nummer ist eine Art Seriennummer des technischen Geräts, die nicht registriert wird. Es handelt es sich also nicht um eine „feste" Beziehung wie zum Beispiel zwischen einem Kfz-Kennzeichen und dem Halter. Eine Beziehung zwischen der MAC-Kennung und personenbezogen Daten lässt sich nicht herstellen. Ein Eingriff in Art. 2 I i.V.m. Art. 1 I GG scheidet demnach auch aus.[116]
Die Feststellung einer Gerätenummer eines W-LAN Gerätes greift demnach nicht in den Schutzbereich eines Grundrechtes ein.
Als Eingriffsgrundlage könnte man an die Befugnisnorm § 100i StPO denken, hierzu müsste eine Analogie gebildet werden. Eine Analogie ist aber nur zulässig, wenn es eine Regelungslücke gibt.[117] Da bei der Ermittlung der MAC-Kennung aber kein grundrechtlich garantierter Schutzbereich tangiert wird, kann der Eingriff auf die allgemeine Eingriffsbefugnis aus §§ 163, 161 StPO gestützt werden.[118]
Die MAC-Nummer ist eine andere Kennung im Sinne von § 100b II StPO und kann damit Grundlage für einen Beschluss nach § 100a StPO sein. Bei der Überwachung eines aktiven W-LAN Gerätes bedarf es genau dieses Beschlusses. [119]
Mangels einer speziellen Eingriffsnorm wie § 100i StPO ist der Zugriff auf die MAC-Kennung nach §§ 163, 161 StPO zulässig.

### 5.7 Beschlagnahme von Datenträgern mit Telekommunikationsdaten

Ist die Telekommunikation in jedem Fall abgeschlossen, ist der Schutzbereich des Fernmeldegeheimnisses aus Art. 10 I GG nicht betroffen. Ein Zugriff auf die archivierten Daten ist ohne weiteres unter den Voraussetzungen der Sicherstellung und Beschlagnahme gemäß §§ 94 ff. StPO möglich. Allerdings ist hierfür eine analogen Anwendung[120] der Vorschriften notwendig, da es nicht um körperliche Gegenstände handelt.

### 5.8 Erhebung von Telekommunikationsverkehrsdaten

Werden von den Strafverfolgungsbehörden nur Informationen über frühere aber auch zukünftige Telekommunikationsverbindungen für die Strafverfolgung benötigt, so können

[115] Demko, NStZ 2004, 57.
[116] Jarass / Pieroth, Art 2, Rn.32.
[117] Larenz / Canaris, Methodenlehre, S. 202.
[118] Gercke, MMR 2003, 453.
[119] Zu allem: Jordan, Bundeskriminalamt – Recht und Polizeipraxis – 2005.
[120] Siehe hierzu: BGH, JuS 2009, 1048; Jahn, JuS 2006, 491; Beulke, §12, Rn. 253b m.w.N..

diese Daten gemäß § 100g StPO erhoben werden.[121] Es handelt sich bei diesen Informationen nicht um Daten, die mit dem Inhalt der Kommunikation übereinstimmen, sondern um die bei der Telekommunikation anfallenden Verkehrsdaten gemäß §§ 96 I und 113a TKG.

Der Ermittlung der Telekommunikationsdaten kommt eine hohe kriminalistische Bedeutung zu. Durch die Daten kann nachvollzogen werden, welche Anschlüsse angewählt worden sind und so lassen sich vor allem im Bereich der BtM-Kriminalität und der organisierten Kriminalität die Strukturen und Spurenansätze herausarbeiten. Durch die Auswertung der mit übermittelten Standortdaten lassen sich Bewegungsprofile erstellen und der Aufenthaltsort des Gerätes ausmachen. Ferner kann das Täterverhalten zur Tatzeit nachvollzogen werden oder durch die Funkzellenabfrage[122] ein Tatort lokalisiert werden. Des Weiteren lassen sich durch die Zielwahlsuche[123] nachträglich die eingegangenen Anrufe zurückverfolgen. Allerdings ist die Zielwahlsuche aufgrund ihrer erheblichen Streubreite nur unter den einschränkenden Bedingungen der Subsidiaritätsklausel des § 100g II StPO zulässig.

Die Verkehrsdaten können auch als Nebenprodukt einer Telekommunikationsüberwachung gemäß §§ 100a, 100b StPO erhoben werden. Die Erhebung dieser Daten, die nicht den Inhalt der Kommunikation betreffen, stellt einen weniger belastenden Eingriff dar, als die eigentliche Überwachung der Kommunikation. Daher haben die §§ 100g, 100h StPO besondere Eingriffsvoraussetzungen mit geringeren Anordnungsvoraussetzungen als Eingriffe nach § 100a StPO.[124] Die Erhebung der Verkehrsdaten in Echtzeit, also nicht die Abfrage von bereits gespeicherten Daten, ist nur nach § 100a StPO zulässig.[125]

Das BVerfG hat in seiner Entscheidung zur Vorratsdatenspeicherung die §§ 113a, 113b TKG für nichtig erklärt. Das Gericht stellte eine Unvereinbarkeit mit Art. 10 I GG fest. Dies hat zur Folge, dass auch § 100g StPO insoweit nichtig ist, als er auf § 113a TKG verweist.[126] Davon nicht betroffen ist hingegen der Rückgriff auf die Verkehrsdaten, die die Telekommunikationsunternehmen nach § 96 I TKG zu Abrechnungszwecken erfasst haben. Unter den Voraussetzungen des § 100g StPO ist ein Zugriff auf diese Daten möglich. Der Verweisung auf § 96 I TKG liegt der allgemeine Gedanke zugrunde, dass Verkehrsdaten, die der Telekommunikationsdienstanbieter für seine vertraglichen Zwecke erheben darf, unter den gesetzlichen Voraussetzungen auch von den Strafverfolgungsbehörden erhoben werden dürfen.[127]

Der Zugriff auf im Endgerät gespeicherte Verkehrsdaten hat über den Weg der Sicherstellung und Beschlagnahme zu erfolgen.

---

[121] Hilger, GA 2002, 557; Zöller, GA 2007, 393; Beulke, §12, Rn. 254a; Keller, TKÜ, S. 23.
[122] Beichel-Benedetti, StV 2005, 438.
[123] BVerfGE 107, 299; zu allem Löffelmann / Walther /Reitzenstein, § 3, Rn. 43, 44.
[124] Löffelmann / Walther /Reitzenstein, § 3, Rn. 38; BVerfGE 107, 299.
[125] Hoeren, JZ 2008, 668.
[126] BK-TKG, Klesczewski, § 113, Rn.1f; BVerfG, NJW 2010, 833.
[127] Welp, GA 2002, 556; Seitz, Strafverfolgungsmaßnahmen im Internet, S170ff..

## 5.9 Bestandsdatenabfrage

Die Erhebung der Verkehrsdaten und die Mobilfunkkennungen wären als solche für die Strafverfolgungsbehörden nutzlos, wenn diese Datensätze nicht mit den personenbezogenen Informationen zusammengeführt werden könnten. Diese sogenannten Bestandsdaten speichern die Kommunikationsanbieter zu Vertragszwecken gemäß § 95 TKG. Für einen Zugriff auf die Daten kann sich die Polizei auf die Ermittlungsgeneralklausel nach §§ 161, 163 StPO berufen. Im Falle des Auskunftsersuchen der Strafverfolgungsbehörden haben die Telekommunikationsanbieter gemäß §§ 111 - 113 TKG die Verpflichtung die entsprechenden Auskünfte zu erteilen.[128]

## 5.10 Sonderfall: Online - Durchsuchung

Unsere gegenwärtige fortschrittsorientierte Gesellschaft ist durch die Nutzung von informatorischen Systemen, insbesondere die Nutzung von PC´S, geprägt. Diese Konzentrierung auf das Internet und den damit verbunden möglichen Diensten birgt allerdings auch einige Gefahren und Probleme für unseren Rechtsstaat. Um diesen Problemen entgegenzutreten hat der Gesetzgeber in jüngster Zeit einige neue Regelungen im Bereich der verdeckten Ermittlungsmaßnahmen geschaffen, die wohl am kontroversesten diskutierten sind die Online - Durchsuchung und die Vorratsdatenspeicherung.
Zu dem Bereich der Online - Durchsuchung können drei verschiedene Konstellationen gezählt werden. Zum einen die Online - Durchsuchung in Form eines „staatlichen Hackings“. Zum Anderen die Durchsuchung von vernetzten Speichermedien und als drittes der Zugriff auf Internet-Telefonie.

### 5.10.1 Online - Durchsuchung

Äußerst heftig umstritten war die Zulässigkeit der sogenannten Online -Durchsuchung, bei der die Ermittlungsbehörden verschleiert die mit dem Internet verbundenen Computer von Tatverdächtigen mittels technischer Vorrichtungen, wie zum Beispiel Trojaner, durchsuchen.[129] Der BGH hat verbindlich festgestellt, dass für den Online - Zugriff auf zugangsgeschützte Bereiche im Internet keine Rechtsgrundlage existiert. Mangels Existenz einer strafprozessualen Eingriffsermächtigung ist eine solche Maßnahme unzulässig und scheidet grundsätzlich aus.[130]
Im Bereich der präventiv-polizeilichen Tätigkeit ist durch den Gesetzgeber in § 20K BKAG eine Ermächtigungsgrundlage zur Online - Durchsuchung[131] geschaffen worden, allerdings ist gegen diese Norm eine Verfassungsbeschwerde anhängig.[132]

---

[128] Vgl. Löffelmann / Walther / Reitzenstein, §3, Rn. 24.
[129] Beulke, §12, Rn.253c; Burmeyer, HRRS 2007, 154.
[130] BGHSt 51, 211; Valerius, JR 2007, 275.
[131] Siehe hierzu umfassend Sparenberg / Heintz, Freilaw Ausgabe 2/2009 S.1.
[132] BVerfG Az.: 1 BvR 966/0; 1 BvR 1140/09 ; Roggan, NJW 2009, 257.

### 5.10.2 Internet / vernetzte Speichereinheiten

Von der Online - Durchsuchung ist die Sichtung eines Computers im Rahmen einer Durchsuchungsmaßnahme durch Ermittlungsbeamte zu unterscheiden, bei der die Beamten mittels Fernzugriff[133] auf einen Rechner oder ein Speichermedium an einem anderen Ort zugreifen. Diese Art der Erkenntnisgewinnung ist durch § 110 III StPO[134] geregelt, teilweise wird die Befugnis auch aus § 100f I Nr.2, §§ 102, 103 StPO gestützt.[135] Voraussetzung ist allerdings, dass ohne die Durchsicht der Verlust beweiserheblicher Daten zu erwarten ist, weil noch vor der körperlichen Sicherstellung des Speichermediums die Löschung der Daten zu befürchten ist.[136] Die Vorschrift des § 110 StPO erfasst alle Gegenstände, die wegen ihres Gedankeninhalts Bedeutung haben, namentlich alle privaten und beruflichen Schriftstücke, aber auch Mitteilungen und Aufzeichnungen aller Art, gleichgültig auf welchen Informationsträger sie festgehalten sind und somit auch alle elektronischen Datenträger und Datenspeicher.[137] Die Durchsicht der als Beweisgegenstände in Betracht kommenden Schriftstücke obliegt der Staatsanwaltschaft. Auf Anordnung durch die Staatsanwaltschaft können Ermittlungspersonen gemäß § 152 GVG die Durchsicht durchführen. Eine Durchsichtsbefugnis bei Gefahr im Verzuge besteht nicht.
Für den Einsatz der sogenannten Polizeistreife im Internet bedarf es keiner besonderen Ermächtigungsgrundlage.[138]

### 5.10.3 VoIP / Internet - Telefonie

In unübersehbarer technischer Nähe zur Online - Durchsuchung steht die Quellen-TKÜ. Hinter dem Begriff der Quellen - TKÜ verbirgt sich der Zugriff auf die Kommunikation,[139] die im Rahmen der Internet Telefonie vollzogen wird. VoIP ist heute für viele PC - Nutzer Alltag geworden. Häufig läuft das Telefongespräch ausschließlich über das Internet, nicht selten mit einer zusätzlichen visuellen Verbindung via Webcam. Das bekannteste Programm hierfür dürfte die kostenlose Software SKYPE sein. Neuere Mobiltelefone bieten mittlerweile auch diese Funktion an.[140]
Für die Strafverfolgungsbehörden ist die Überwachung und Auswertung der VoIP - Kommunikation allerdings mit einigen Schwierigkeiten verbunden. Eine Telekommunikationsüberwachung ermöglicht zwar eine Aufzeichnung sämtlicher Verkehrs- und Inhaltsdaten, dessen ungeachtet verschlüsseln nahezu alle VoIP - Produkte den digitalisierten Datenstrom mittels mathematischer Verfahren. So ist die vollständige

[133] Beulke, §12, Rn. 253c.
[134] Schlegel, HRRS 2008, 23.
[135] Löffelmann / Walther / Reitzenstein, §3, Rn. 37.
[136] Meyer-Goßner, §110, Rn.6, 7.
[137] BGH, NJW 1995, 3397; BGH, CR 1999, 292.
[138] Siehe hierzu vertiefend: Zöller, GA 2000, 563; KK-Nack, §98a, Rn. 33.
[139] Becker / Meinicke, StV 2011, 50.
[140] Technische Grundlagen siehe: Sankol, CR 2008, 13.

Wiederherstellung und Lesbarkeit der Kommunikation nur mittels der Kenntnis um den entsprechenden Schlüssel möglich. Die erlangten Daten sind im Rahmen einer herkömmlichen TKÜ folglich zunächst wertlos.
Zur Lösung dieses Problems erfolgt der Zugriff auf die Daten an der „Quelle“. Das bedeutet, dass auf ein Endgerät eines Kommunikationsteilnehmers zugegriffen wird bevor die Daten verschlüsselt oder nachdem die Daten entschlüsselt worden sind. Allen Verfahren, die das Abfangen der Daten ermöglichen, ist gemeinsam, dass sie auf dem Zielsystem eine Software installieren und so mittels Spionagesoftware[141] das System infiltrieren.[142] Auf diesem Weg ist die Aufzeichnung und Übermittlung von unverschlüsselten Daten möglich. Diese unübersehbare technische Nähe und Verfahrensweise der Quellen-TKÜ zur nicht zulässigen Online - Durchsuchung wirft die Frage auf, ob es eine strafprozessuale Ermächtigungsgrundlage gibt. In Betracht kommen könnte § 100a StPO.
Das BVerfG hat in seiner Entscheidung gegen die Zulässigkeit der Online -Durchsuchung klargestellt, dass bei solchen Maßnahmen, das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informatorischer Systeme zu beachten ist.[143] Des Weiteren darf nicht in den Kernbereich der privaten Lebensgestaltung eingegriffen werden. Es darf dementsprechend bei der Quellen-TKÜ nicht zu einem Zugriff auf andere als die Kommunikationsdaten kommen. Durch die Infiltration des Zielsystems kommt es zu einer Gefährdungslage, der nicht alleine Art. 10 GG Rechnung tragen kann, da nur die Telekommunikationsfreiheit geschützt wird. Art. 10 GG und § 100a StPO können nur dann die relevanten Normen sein, wenn sichergestellt ist, dass nicht auf andere Daten als die Kommunikationsdaten des laufenden Kommunikationsvorgangs zugegriffen wird und werden kann.[144]
Es ist streitig, ob § 100a StPO ausreicht, um auf VoIP – Kommunikation zugreifen zu können oder nicht. Nach der im Moment wohl herrschenden Meinung erscheint die Auswertung der abgefangen Daten gemäß § 100a StPO als richtig.[145]
Der Meinung folgend ist die Primärmaßnahme, die Gesprächsüberwachung, nach § 100a StPO zulässig. Fraglich ist allerdings, ob die technische Durchführung auch noch unter § 100a StPO möglich ist. Dies wäre nur zulässig, wenn man die Sekundärmaßnahme, die Installation des Spionageprogramms, als eine Annexkompetenz zu der Telekommunikations-überwachung ansieht. Dies ist indessen nur dann der Fall, wenn sichergestellt ist, dass keine technische Zugriffs- bzw. Kenntnisnahmemöglichkeit von Daten ermöglicht ist, die über die Daten des Kommunikationsvorgangs hinausgehen. Sollte diese Voraussetzung nicht zu

[141] Backdoor-Programm, Trojaner.
[142] KK-Nack, §100a, Rn. 27; AG Bayreuth, MMR 2010, 266; LG Hamburg Az: 608 Qs 17/10; LG Landshut Az: 4 Qs 346/10.
[143] BVerfGE 120, 274.
[144] Meyer-Goßner, §100a, Rn.7; kritisch Becker / Meinicke, StV 2011, 50 m.w.N..
[145] Roxin / Schünemann, §36, Rn.1; KK-Nack, §100a, Rn.27; a.A SK-StPO, Wolter, §100a, Rn.27ff.; BVerfGE 120, 274; zum Streitstand siehe: Becker / Meinicke, StV 2011, 50.

erfüllen sein, handelt es sich faktisch um eine Online - Durchsuchung, die nicht zulässig ist.[146] Zu vernachlässigen ist auch nicht, ob durch den Zugriff auf das Zielsystem Art. 13 GG betroffen ist, da ein Eindringen in die Wohnung des Betroffen in irgendeiner Form vorliegt.[147] Eine Überwachung von verschlüsselter Internet-Telefonie ist ohne eine technische Begrenzung, die den verfassungsrechtlichen Anforderungen genügt, mangels einer genügenden Ermächtigungsgrundlage derzeit nicht zulässig. Sofern sich die Überwachung ausschließlich auf Daten der laufenden Telekommunikation beschränkt, bildet § 100a StPO eine Eingriffsgrundlage.

### 5.11 Mauterfassung

Im Rahmen der Mauterfassung finden zahlreiche Vorgänge statt, die in den Komplex der Telekommunikation fallen. Vorstellbar wäre eine Auswertung der Daten im Rahmen der Vorschriften der StPO. Allerdings dürfen die Informationen, die im Rahmen des Mauterfassungssystems auf den Autobahnen erfasst werden, gemäß §§ 4 II, 7 II ABMG ausschließlich zum Zwecke der Mauterhebung verwendet werden. Eine ausnahmsweise Verwendung der Daten zum Zwecke der Strafverfolgung ist nicht zulässig.[148]

### 5.12 Zusammenfassung

Die Überwachung des Fernmeldeverkehrs stellt einen umfassenden und schwerwiegenden faktischen Eingriff in das Fernmeldegeheimnis im Sinne des Art. 10 GG und durch die die Erhebung personenbezogener Daten in das Grundrecht auf informationelle Selbstbestimmung im Sinne des Art. 2 I GG i.V.m. Art. 1 GG dar. Daraus ergeben sich zahlreiche Probleme, die eine umfassende Kenntnis der Eingriffsvoraussetzungen erfordert und eine konkrete Bestimmung des Eingriffszieles, um alle materiellen und formellen Voraussetzungen zu erfüllen und ein Beweiserhebungs- oder Beweisverwertungsverbotes zu verhindern.

## 6 Grenzen der Beweissammlung im Strafverfahren

Mit der ursprünglichen Straftat entsteht der staatlich Strafanspruch gegen den Täter. Das materielle Strafrecht bestimmt die Voraussetzungen für das Entstehen des Strafanspruchs. Wie eine Straftat verfolgt wird, welche Maßnahmen zur Erforschung und Urteilsfindung zulässig sind, ist im Strafverfahrensrecht geregelt. Im Strafverfahrensrecht ist das Erforschen und Ahnden von Straftaten geregelt.
Das wesentliche Ziel des strafprozessualen Ermittlungsverfahrens ist in der Erforschung der Wahrheit zu sehen. In diesem Sinne gibt § 160 II StPO der Staatsanwaltschaft auf, nicht nur

[146] KK-Nack, §100a, Rn.27; Beulke, § 12, Rn. 253c; Ruhmannseder, JA 2009, 57.
[147] Siehe hierzu: Böckenförde, JZ 2008, 925.
[148] Vertiefend siehe hierzu: Bosch, JA 2006, 747; Göres, NJW 2004, 195.

zur Belastung, sondern auch zur Entlastung dienenden Umständen zu ermitteln. Der Sachverhalt ist demzufolge umfassend aufzuklären. Die Zielbestimmung der Wahrheitsfindung kann den Charakter des Ermittlungsverfahrens jedoch nur teilweise erfassen. Denn das Ermittlungsverfahren bezweckt nicht eine Wahrheitsermittlung um jeden Preis. Vielmehr müssen grundrechtlich verbürgte Interessen im Spannungsverhältnis von Sicherheit und Freiheit abgewogen werden.[149]

Beweisverbote sind das Werkzeug zur Sicherung von Individualinteressen, die sich der Staat selbst auferlegt hat. Sie beruhen auf der Überlegung, dass der durch den Strafprozess beabsichtigte Rechtsgüterschutz durch die mit ihm zwangsläufig verbundenen Eingriffen nicht überwogen werden soll.

Es ist zu unterscheiden zwischen Beweiserhebungs- und Beweisverwertungsverboten. Die Beweiserhebungsverbote sollen eine unverhältnismäßige oder schlechthin unzulässige Beeinträchtigung schutzwürdiger Rechtsgüter von vorneherein verhindern. Die Beweisverwertungsverbote sind gekennzeichnet von der Frage, ob bestimmte Beweise im Rahmen eines Strafverfahrens durch das Gericht zur Begründung eines Schuldspruches herangezogen werden dürfen, wenn die Erkenntnisgewinnung in Bezug auf diese Beweise rechtswidrig erfolgt ist.[150]

## 6.1 Beweiserhebungsverbote

Der Wahrheitserforschung hat der Gesetzgeber bewusst Grenzen gesetzt. Diese Schranken bestehen zunächst in den materiellen und formellen Voraussetzungen der entsprechenden Ermächtigung der Eingriffe. So zum Beispiel in dem abschließend aufgelisteten Katalog der Anlassstraftaten in § 100a StPO.[151]

Die Beweiserhebungsverbote gliedern sich zunächst in:

**Beweisthemaverbote:** Durch sie wird die Aufklärung bestimmter Sachverhalte untersagt. Beispielsweise die Erlangung von Erkenntnissen aus dem Kernbereich der persönlichen Lebensgestaltung bei der Telekommunikationsüberwachung.

**Beweismittelverbote:** Sie untersagt die Verwendung bestimmter Beweismittel. Beispielhaft hierfür sind aussage- und untersuchungsverweigerungsberechtigte Personen, die von ihrem Recht gebrauch machen.

**Beweismethodenverbote:** Diese schließen eine bestimmte Art der Beweisgewinnung aus, zum Beispiel der Einsatz unzulässiger Vernehmungsmethoden gemäß § 136a I, II StPO.[152]

[149] Roxin / Schünemann, §2, Rn.1; Löffelmann / Walther / Reitzenstein, §1, Rn. 49.
[150] Löffelmann / Walther / Reitzenstein, §6, Rn. 3.
[151] Eckhardt, CR 2007, 337.
[152] Beulke, § 23, Rn. 455; Löffelmann / Walther / Reitzenstein, §6, Rn. 3.

Für den Bereich der Telekommunikationsüberwachung sieht das Strafverfahrensrecht in § 100c IV und VI StPO und in § 100h II StPO Beweiserhebungsverbote vor. Diese expliziten Beweiserhebungsverbote sind Ausnahmen im Strafverfahrensrecht. Es handelt sich um Beweisthemaverbote. Hinzu kommt der Schutz von Berufsgeheimnisträgern. Sofern sie nicht Zielperson einer Überwachungsmaßnahme als Beschuldigter sind, ergeben sich aus § 160a I S.1-4, II StPO Beweiserhebungsverbote und Beweisverwendungsverbote, einschließlich Verwertungsverbot sowie Dokumentations- und Löschungspflichten.[153]
Bei heimlichen Ermittlungsmaßnahmen kommt dem Schutz des Kernbereichs der privaten Lebensgestaltung besondere Bedeutung zu.[154] Zunächst ist somit die Frage zu beantworten, wann der Kernbereich betroffen ist.

### 6.1.1 Bestimmung des Bereichs der privater Lebensgestaltung

In den Kernbereich der privaten Lebensgestaltung darf nicht eingegriffen werden. Der § 100a IV StPO enthält ein gesetzliches, ausdrückliches Erhebungs- und Verwertungsverbot für Kommunikationsinhalte aus dem intimsten Bereich. Folglich ist die Überwachung der Telekommunikation, wenn über innerste Gefühle und höchstpersönliche Überlegungen gesprochen wird, nicht zulässig. Erfolgt dennoch eine Überwachung, dürfen die aus der Kommunikation gewonnen Erkenntnisse keinesfalls in einem Strafverfahren verwertet werden.[155]
§100 a IV StPO enthält Regelungen, die dem Schutz des Kernbereichs privater Lebensgestaltung dienen und verhindern sollen, dass Erkenntnisse aus diesem Bereich erlangt oder zumindest verwertet werden. Die Vorschrift trägt der Entscheidung des BVerfG Rechnung, wonach verdeckte, heimliche Überwachungsmaßnahmen staatlicher Stellen einen unantastbaren Kernbereich privater Lebensgestaltung zu wahren haben, dessen Schutz aus Art. 1 GG hergeleitet wird. Selbst überwiegende Interessen der Allgemeinheit können einen Eingriff in den Kernbereich nicht rechtfertigen.[156]
Die Frage, wann der Kernbereich der privater Lebensgestaltung betroffen ist, kann nur im Einzelfall beantworten werden, da bisher weder durch den Gesetzgeber noch durch die Rechtsprechung eine feste Begriffsbildung gebildet worden ist.[157]
Dem absoluten Schutz unterfallen vor allem Vorgänge, die das Wesen der jeweiligen Persönlichkeit in ihrem Innersten offenbaren. Der Kernbereich privater Lebensgestaltung ist jedoch erst dann tangiert, wenn das überwachte Gespräch tiefste innere Vorgänge

[153] Harnisch / Pohlmann, HRRS 2009, 202.
[154] BVerfG, NJW 2005, 2603.
[155] BGH, StraFo 2009, 19; Baldus, JZ 2009, 218.
[156] Detterbeck, ÖR, Rn. 493ff..
[157] BGH, JR 1994, 430; Beulke, § 23 Rn. 471.

privatester Natur offenbart, was eine enge Auslegung nahe legt. Als Faustformel kann gelten: *„Wenn das Innerste nach außen gekehrt wird“.*[158]
Entscheidend für die Beurteilung ist zunächst, ob die Kommunikation nach ihrem Inhalt aufgrund von konkreten Hinweisen oder typischerweise höchstpersönlichen Charakter hat und in welcher Art und Intensität die Sphäre anderer oder Belange der Gemeinschaft durch die Telekommunikation berührt werden. Als ergänzendes Indiz kommt die konkrete Kommunikationssituation hinzu. Wenn nach der inhaltlichen Prüfung die Möglichkeit besteht, dass es eine Kernbereichsrelevanz gegeben sein könnte, kann die Gesamtbetrachtung von Kommunikationsinhalt und Kommunikationssituation entscheidend sein. Wichtige Parameter sind hier das Vertrauensverhältnis der kommunizierenden Personen, die Örtlichkeit der Kommunikation, Ausmaß und Art der geäußerten Gefühle, der Wille die höchstpersönlichen Äußerungen geheim zu halten und die Tatsache, dass die Gesamtumstände der Kommunikation Rückschlüsse darauf zu lassen, dass die Kommunikationsteilnehmer subjektiv die geführte Kommunikation dem Kernbereich zugerechnet haben wollen.[159]
Die TKÜ darf nicht angeordnet werden, wenn von Anfang an tatsächliche Anhaltspunkte vorliegen, dass ausschließlich Erkenntnisse aus dem Kernbereich privater Lebensgestaltung zu erwarten sind.[160]
Zum Schutz von zeugnisverweigerungsberechtigten Personen bei allen Ermittlungsmaßnahmen verweist § 160 a StPO ausdrücklich auf die §§ 53, 53a, 97 und 100c VI StPO. Diese Spezialvorschriften gehen den Allgemeinen vor, im Übrigen bleiben die Erhebungsvorschriften des § 160 a StPO anwendbar.[161]
Aus der Erscheinungsform der gesetzlich geregelten Beweisverbote kann man nicht auf Willkür beim Gesetzgeber bei deren Schaffung schließen. Zwar ist kein einheitliches Gesamtkonzept zu erkennen. So sind dem Gesetzgeber aber bereits durch die Verfassung Grenzen gesetzt.

### 6.1.2 Verfassungsrechtliche Beweiserhebungsverbote

Im Einzelfall können sich Beweiserhebungsverbote auch ausnahmsweise unter strengen Voraussetzungen direkt aus der Verfassung ergeben. Alle staatlichen Maßnahmen dürfen demzufolge nicht in den durch die Menschenwürde geschützten unantastbaren Bereich der höchstpersönlichen Lebensgestaltung eingreifen.[162]
Auch können sich Beweisverbote unmittelbar aus dem verfassungsmäßigen Verhältnismäßigkeitsgrundsatz ergeben. Der Grundsatz der Verhältnismäßigkeit bindet alle

[158] BVerfGE 80, 367; BVerfGE 34, 238; Baldus, JZ 2008, 218.
[159] Meyer-Goßner, § 100a, Rn. 24a; BVerfG, NJW 2004, 999.
[160] Bär, MMR 2008, 215; Rogall, JZ 2008, 818.
[161] Barton, JZ 2010, 102; ebenso: Glaser / Gedeon, GA 2007, 415.
[162] BVerfGE 34, 238; BVerfGE 109, 279; Löffelmann, ZStW 2006, 358; vgl. auch Löffelmann / Walther / Reitzenstein, §3, Rn. 21.

staatliche Gewalt, sofern staatliche Hoheitsträger subjektiv die Rechte eines Bürgers in irgendeiner Weise beeinträchtigen. Dies kommt stets dann in Betracht, wenn auf Grund der Eigenart des Beweisthemas in den grundrechtlich geschützten Bereich unter dem Grundsatz der Verhältnismäßigkeit eingegriffen wird. Der Eingriff muss in einem angemessenen Verhältnis zu dem Gewicht und der Bedeutung des Grundrechts stehen.[163]
Es darf nicht eine Wahrheitserforschung um jeden Preis betrieben werden. Vielmehr muss die Werteordnung, die durch das Grundgesetz festgelegt ist, mit dem Strafverfolgungsinteresse im Einklang stehen. Insofern sind die dem staatliche Handeln durch die Grundrechte gezogenen Schranken auch von den Strafverfolgungsbehörden zu beachten. Hierbei ist insbesondere an den aus Art. 2 I i.V.m. 20 III GG abgeleiteten Anspruch auf ein rechtstaatliches faires Verfahren zu denken.[164] Dies hat zur Folge, dass nicht alle Beweise erhoben werden dürfen, da Rechtsgüter und höherwertige Interessen dem entgegenstehen.
Dieser Grundsatz findet auch in § 100c V StPO Anwendung. Durch diese Regelung wird gerade der Kernbereich der privaten Lebensgestaltung geschützt. Dies kann unter Umständen soweit gehen, dass die Überwachung unterbrochen werden muss.

Eine allgemeine Regel, wann die Verletzung eines Beweiserhebungsverbotes zu einem Beweisverwertungsverbot führt, konnte bisher allerdings nicht entwickelt werden.[165]

### 6.2 Beweisverwertungsverbote

Ist bei der Erhebung eines Beweises ein Fehler unterlaufen, so stellt sich die Frage, ob dies zu einem Beweisverwertungsverbot für das Verfahren führt. Wenn die Erkenntnisse den Ermittlungsbehörden bereits zur Verfügung stehen, läuft der Schutzzweck von Beweiserhebungsverboten, eine Rechtsgutsverletzung bei dem von den Ermittlungen Betroffenen zu verhindern, ins Leere. Daher stellt sich die Frage ob, rechtswidrig erlangte Beweise verwertet werden dürfen. Beweisverwertungsverbote schließen bestimmte Beweisergebnisse von der Berücksichtigung im Verfahren aus. Sofern bezüglich eines Beweismittels ein Beweisverwertungsverbot eingreift, ist dies umfassend und darf auch nicht durch Rückgriff auf ein anderes Beweismittel umgangen werden. Außerhalb der gesetzlichen geregelten Beweisverwertungsverbote muss dies durch Wertung ermittelt werden. Dies kann mittels der Rechtskreistheorie oder der Abwägungslehre erfolgen.[166]
Ausgehend von der Rechtskreistheorie, wonach das unter einem Verfahrensverstoß gewonnen Beweismittel unverwertbar ist, wenn die verletzte Vorschrift wesentlich dem Schutz des Rechtskreises des Beschuldigten dient, wird in Erweiterung dieser Theorie

[163] Jarass / Pieroth, Art.20, Rn. 81, 86 beachte hierzu: BGHSt 43, 300; BVerfG, NStZ-RR 2004, 83.
[164] Beulke, § 23, Rn. 454; BVerfGE 86, 288.
[165] Vgl. Beulke, § 23, Rn. 457; Eisenberg, Rn. 370.
[166] Schroth, JuS 1998, 969.

zusätzlich eine Abwägung im Einzelfall vorgenommen. Hierbei sind insbesondere der Regelungszweck der Verletzten Vorschrift, die sich aus dem Grundgesetzt ergebene Wertigkeit der widerstreitenden Interessen im Einzelfall sowie der Verhältnismäßigkeitsgrundsatz zu berücksichtigen. Bei jedem rechtswidrigen Eingriffsakt ist durch eine umfassende Wertung mittels der erweiterten Rechtskreistheorie bzw. der Abwägungslehre zu ermitteln, ob hieraus ein Verwertungsverbot resultiert.[167]
Allgemein lässt sich feststellen, dass die Rechtsprechung bei der Wertung zurückhaltend vorgeht und grundsätzlich ein Verwertungsverbot nur bei besonders schweren oder willkürlichen Verstößen annimmt. Häufig wird ein Verwertungsverbot auch damit begründet, dass das Beweismittel durch einen hypothetischen Ersatzeingriff auch hätte rechtmäßig erlangt werden können.

### 6.2.1 Gesetzliche Beweisverwertungsverbote

Es gibt nur wenige gesetzlich geregelte Beweisverwertungsverbote, daher ist für die Lehre der Beweisverwertungsverbote überwiegend von der Rechtsprechung geprägt. Im Bereich der Telekommunikationsüberwachung gibt es Regelungen in § 100c und § 100h StPO. § 100c V StPO regelt die Folgen eines Eingriffs in den Kernbereich der privaten Lebensgestaltung. Jede Verwertung kernbereichsrelevanter Gespräche ist ausgeschlossen und zwar nicht nur für das betriebene Verfahren, sondern auch als Spurenansatz.[168] In § 100h StPO wird der Einsatz weiterer technischer Mittel außerhalb der Wohnung geregelt. Soweit der Kernbereich der privaten Lebensgestaltung nicht tangiert ist, sind die erlangten Erkenntnisse uneingeschränkt verwertbar.[169]
Verfassungsrechtliche Verwertungsverbote, können sich wie bei den Erhebungsverboten, durch den Eingriff in den Kernbereich privater Lebensgestaltung und den daraus gewonnen Erkenntnissen ergeben.

### 6.2.2 Nicht normierte Verwertungsverbote

Das Vorliegen eines Beweisverwertungsverbotes ist nicht von dessen ausdrücklicher Normierung abhängig. Grundsätzlich gilt nach der Rechtsprechung[170], dass Verfahrensfehler bei der Beweiserhebung nicht zwangsläufig ein Verwertungsverbot zur Folge haben. Die Rechtsprechung wertet im Rahmen der Abwägungslehre jeden Einzelfall für sich. Die Entstehung eines Verwertungsverbotes hängt also von der Abwägung zwischen der Bedeutung des in Rede stehenden Beweismittels für das Strafverfahren und der Schwere des Verstoßes gegen die Erhebungsvorschrift ab. Die Rechtskreistheorie hat sich in der Rechtsprechung nur für den Bereich des § 55 StPO durchgesetzt. Eine einheitliche und

[167] BGHSt 11, 213; BGH, NJW 1999, 959.
[168] Rogall, JZ 2008, 818; BGH, NJW 2009, 3448.
[169] Rogall, JZ 2008, 818; Meyer-Goßner, § 100c, Rn.17; § 100h, Rn. 12.
[170] Beispielhaft für viele: BGHSt 38, 214; 44, 243.

konsequente Linie ist in den zahlreichen Entscheidungen nicht zu erkennen.[171] In jüngeren Entscheidungen ist dem hypothetischen Ersatzeingriff eine immer größere Bedeutung zugekommen. Mit der Anwendung des Ersatzangriffes schafft die Rechtsprechung den Strafverfolgungsbehörden einen relativ großen Spielraum und ermöglicht die Verwertbarkeit von rechtswidrig erhobenen Erkenntnissen. Im Ergebnis werden so Verfahrensfehler bei der Beweiserhebung geheilt und abgefedert. Verfahrensfehler können so nicht das gesamte Strafverfahren lahm legen.

### 6.2.3 Zufallsfunde

Eine herausragende Problemstellung im Bereich des § 100a StPO bilden die Zufallsfunde. Unter Zufallsfunden sind Erkenntnisse zu verstehen, die nichts mit der Tat, wegen derer die Anordnung ergangen ist, zu tun haben. Sie beziehen sich auf eine ganz andere Straftat. Zunächst muss erst einmal dazwischen unterschieden werden, ob die Erkenntnisse sich auf eine Katalogstraftat oder eine andere Straftat beziehen. Diese andere Straftat müsste in einem unmittelbaren Zusammenhang mit einer Katalogstraftat stehen.[172] Sollte dies gegeben sein, sind die gewonnen Erkenntnisse verwertbar zu Beweiszwecken, sofern die Telekommunikationsüberwachung rechtmäßig angeordnet wurde. Für alle übrigen Fälle gilt ein Verwertungsverbot, dass auf einer nicht unzulässigen Beweisgewinnung beruht. Die herrschende Rechtsprechung schließt durch das Verwertungsverbot allerdings nicht aus, dass die gewonnen Erkenntnisse als Spur weiterverfolgt werden und so andere Beweismittel gewonnen werden können.[173] Eine weitere Verwertung als Spurenansatz ist nach Meinung der Rechtsprechung möglich. Der überwiegende Teil der Literatur lehnt dies allerdings nach den allgemeinen Regeln der Fernwirkung von Beweisverwertungsverboten ab.

### 6.2.4 „fruit of the poisonous tree doctrine“ / Fernwirkung

Die Reichweite der Beweisverwertungsverbote ist umstritten. Fraglich ist, ob den Beweisverwertungsverboten eine Fernwirkung zukommt. Sind Ermittlungsergebnisse, die auf Grund eines einem Verwertungsverbot unterliegenden Beweises gewonnen wurden, ebenfalls von einem Verwertungsverbot betroffen? Dies könnte zum Beispiel bei der Preisgabe des Verstecks eines Entführungsopfers unter Verwendung nicht zulässiger Vernehmungsmethoden der Fall sein.[174]
Die Rechtsprechung hat bisher für alle Verstöße gegen ein Verwertungsverbot eine Fernwirkung verneint.
Dies wurde damit begründet, dass nicht ein Verfahrensverstoß das gesamte Strafverfahren lahm legen dürfe und sich kaum jemals feststellen lasse, ob die Ermittlungspersonen das

[171] Zu allem: Beulke, §6, Rn. 14 m.w.N. vor allem die Rechtsprechung des BGH.
[172] Kretschmer, StV 1999, 221; BGHSt 27, 355.
[173] Allgayer, NStZ 2006, 603.
[174] BGH, NJW 2006, 1361; BVerfG, NStZ 2006, 46.

weitere Beweismittel nicht auch ohne den gerügten vorhergehenden Verfahrensverstoß gewonnen hätten. Das Verwertungsverbot schließt demzufolge nicht aus, dass gewonnene und nicht verwertbare Beweise im Rahmen des Spurenansatzes weiterverfolgt und genutzt werden können und dabei neue andere Beweismittel gewonnen werden.[175] Eine abweichende Entscheidung hat der BGH bisher nur zu § 7 III G10 getroffen und diesem eine Fernwirkung zugebilligt.[176]

Eine weitere Meinung (Funktionslehre) befürwortet, in Anlehnung an die amerikanischen *„fruit oft the poisonous tree doctrin“* Theorie, die Fernwirkung von Verwertungsverboten. Die Beweise, die auf Grund eines Verfahrensverstoßes erlangt wurden, sollen auch dazu führen, dass die mittelbar daraus gewonnen weiteren Erkenntnisse einem Verwertungsverbot unterliegen, da sonst der Sinn und Zweck der Beweisverwertungsverbote unterlaufen werde.[177]

Eine dritte vermittelnde Meinung (Schutzzwecklehre) befürwortet die Lösung im Rahmen einer Einzelfallbewertung durch eine Abwägung zwischen dem Gewicht des ursprünglichen Verfahrensverstoßes und der Schwere der verfolgten Straftat.[178]

Sinnvoll und richtig erscheint es, mit der vermittelnden Meinung, auf den Schutzbereich der verletzten Strafverfahrensnorm abzustellen und eine Gesamtabwägung zwischen der begangenen Rechtsverletzung und der Bedeutung des Tatvorwurfes vorzunehmen. Dabei sind allerdings vor allem zwei Aspekte immer besonders zu berücksichtigen. Zum einen, dass die durch den Verfahrensverstoß erlangten Erkenntnisse, den eigentlichen Rechtsbruch noch weiter intensivieren. Und im Rahmen des hypothetischen Ersatzeingriff zum anderen, ob die rechtswidrige Beweisverwertung dadurch legitimiert werden kann, dass die Ermittlungsorgane, bei einem rechtmäßigen Vorgehen ein identisches Beweisergebnis erzielt hätten.[179]

### 6.2.5 Geltendmachung von Verwertungsverboten

Ob ein vorhandener Verfahrensfehler ein Verwertungsverbot begründet, hängt maßgeblich von der Sachverhaltskenntnis der zuständigen, die Eingriffsmaßnahme anordnenden Stelle und deren Beurteilung ab. Die Verwertbarkeit ist vom Gericht von Amts wegen umfassend zu prüfen. Allerdings vertritt die Rechtsprechung[180] die Widerspruchslösung, nach der es dem Angeklagten obliegt, der Verwertung zu widersprechen.

Eine Prüfung erfolgt demnach nur, wenn der Verwertung rechtzeitig widersprochen worden ist. Rechtzeitig bedeutet unmittelbar nach dem Ende der Beweiserhebung gemäß § 257

[175] Allgayer, NStZ 2006, 603.
[176] Siehe hierzu BGHSt 29, 244.
[177] Müssig, GA 1999, 119.
[178] Maiwald, JuS 1978, 379; Meyer-Goßner, Einl., Rn.57.
[179] Zu allem: Beulke, § 23, Rn. 482; Meyer-Goßner, § 136a, Rn. 31.
[180] BGH 38, 214; 42, 15.

StPO.[181] Diese Widerspruchslösung wurde zunächst nur für Verstöße gegen Belehrungspflichten entwickelt, ist aber mittlerweile nach herrschender Meinung auf alle Verwertungsverbote, die auf der Verletzung von Individualrechten beruhen, an zuwenden.[182] Die Entwicklung der Widerspruchslösung ist von dem Gedanken getragen, dass dem Beschuldigten und seiner Verteidigung eine Dispositionsmacht über die Beweise eingeräumt werden soll. Kritik an der Widerspruchslösung zielt vor allem darauf ab, das der Verteidigung gerichtliche Aufklärungs- und Fürsorgepflichten übertragen wird. Dies führt ohne gesetzliche Grundlage zur Unbeachtlichkeit schwerster Verfahrensfehler und verletzt so das Recht des Angeklagten auf ein faires Verfahren.[183] Das BVerfG hält die Widerspruchslösung nichtsdestotrotz für verfassungskonform. Zumal auf diesem Weg dem Angeklagten eine Verfügungsgewalt über die Verwertbarkeit der Beweismittel zugestanden wird und sich so für ihn durchaus Spielräume bei der Verteidigungsstrategie im Rahmen der Beweisaufnahme ergeben.

Nach erfolgtem rechtzeitigem Widerspruch, obliegt die endgültige Entscheidung, ob ein Verwertungsverbot eintritt, dem erkennenden Gericht.

Erkenntnisse aus einer Telekommunikationsüberwachung gemäß § 100a StPO sind ausnahmslos unverwertbar, wenn sie materielle Voraussetzungen für die Überwachung nicht erfüllen. Dies ist insbesondere dann der Fall, wenn kein Verdacht auf eine Katalogstraftat vorlag, das Subsidiaritätsprinzip verletzt wurde oder aber die Überwachung aus einem anderen Grund unzulässig war. Bei der Beurteilung der materiellen Voraussetzungen steht der zuständigen Staatsanwaltschaft allerdings ein Ermessensspielraum zu.[184] Zu einem Verwertungsverbot soll es daher nur kommen, wenn objektiv Willkür oder eine grobe Fehlbeurteilung der Rechtslage vorliegt.

Heilbar sein soll ein Verstoß gegen die Voraussetzung, dass die Anordnung nur für eine Katalogstraftat ergehen darf. Die Anordnung der Maßnahme also nicht für eine Anlasstat ergangen ist. Gleichzeitig zu dieser Straftat muss allerdings noch der Verdacht auf eine Katalogstraftat vorgelegen haben, die die Anordnung gerechtfertigt hätte.[185] Eine Wertung erfolgt im Rahmen der hypothetischen Kausalität.

Liegen die Voraussetzungen der §§ 100b, 101 StPO, die formellen Voraussetzungen, nicht vor, kommt es nur in Ausnahmefällen zu einem Verwertungsverbot. Ein Verstoß gegen die formellen Voraussetzungen führt nur bei nicht Beachtung des § 100b I StPO zu einem Verwertungsverbot, da die gerichtliche oder staatsanwaltliche Anordnung gänzlich fehlt.

[181] Löffelmann / Walther / Reitzenstein, §6, Rn. 28.
[182] Gaede, HRRS 2007, 402; BGHSt 38, 214; BGHSt 42, 15; Meyer-Goßner, § 136, Rn. 25.
[183] Roxin / Schünemann, §24 Rn.34; Beulke, § 23, Rn. 460a.
[184] Beulke, § 23 Rn. 475; siehe hierzu Meyer-Goßner, §337, Rn. 17; KK-Kuckein, § 337,Rn. 16ff..
[185] Kinzig, StV 2004, 560; Kudlich, JR 2003, 453.

Ebenso führt die Entscheidung eines unzuständigen Richters zu einem Verwertungsverbot.[186]
Von den Beweisverwertungsverboten sind die Verwendungsverbote zu unterscheiden. Die Grundsätze, die die Rechtsprechung für die Beweisverwertungsverbote entwickelt hat, nach denen ein Verstoß bei der Beweiserhebung zu einem Verwertungsverbot führt, gelten auch für Verwendungsregelungen und Verwendungsbeschränkungen.[187] Ob ein Verwertungs- und Verwendungsverbot vorliegt, hängt maßgeblich von der Bewertung des Einzelfalles ab. Festzuhalten bleibt aber ein absolutes Verwertungsverbot, sobald der Kernbereich privater Lebensgestaltung tangiert ist.

## 7 Fazit

Grundsätzlich gilt es von staatlicher Seite in der Abwägung zwischen der effektiven Strafverfolgung und dem Eingriff in grundgesetzlich garantierte Rechte ein besonderes Maß an Sensibilität zu zeigen. Gerade aufgrund der Eingriffstiefe von Maßnahmen der Telekommunikationsüberwachung stellt sich die Frage nach dieser Abwägung.
Leider ist festzustellen, dass es in NRW keine Regelungen zur präventiven TKÜ gibt, so dass immer über den grenzwertigen Weg der Umwidmung der Daten eine Möglichkeit zur Nutzung geschaffen werden muss. Es wäre zu befürworten, dass eine solche Regelung, die den verfassungsrechtlichen Ansprüchen genügt, geschaffen wird.
Sowohl durch die Justiz als auch durch die Strafverfolgungsbehörden und verschiedene Forschungseinrichtungen wird dokumentiert, dass es sich bei der Telekommunikationsüberwachung um eine wichtige und Erfolg versprechende Ermittlungsmethode handelt. Die Telekommunikationsüberwachung ist im Zeitalter zunehmender Kommunikation, in aller ihrer Vielfalt, eine für das strafrechtliche Ermittlungsverfahren überaus bedeutsame Erkenntnisquelle. Die gilt insbesondere für Verfahren im Zusammenhang mit der Bekämpfung des internationalen Terrorismus, der Bekämpfung der organisierten Kriminalität und BtM-Kriminalität.
Der Vorteil der Telekommunikationsüberwachung gegenüber der offenen Ermittlungsarbeit liegt zweifelsfrei darin, dass der Beschuldigte von der gegen ihn gerichteten Maßnahme keine Kenntnis hat und dass er daher sehr wahrscheinlich unbefangen Äußerungen tätigt, die direkt oder mittelbar, gegen ihn verwendet werden können.[188]
Die eingesetzten Ermittlungspersonen, sowohl von Polizei als auch von Justiz müssen ein umfassendes Wissen über die Regelungen bezüglich der Sicherstellung und Beschlagnahme haben, um abgrenzen zu können, ab wann TKÜ-Regelungen einschlägig sind, da sonst Verwertungsverbote und Verwendungsverbote drohen. Dies hätte zur Folge,

[186] Beulke, § 23 Rn. 476; Malek / Wohlers, Rn. 446.
[187] Siehe hierzu BGH 54, 69; Meyer-Goßner, Einl., Rn.57e.
[188] Siehe hierzu: Füllkrug, Kriminalistik 1990, 349.

dass unter Umständen das Strafverfahren scheitert und gegebenenfalls auch weitere Spurenansätze nicht verwertet werden dürfen. Dies verlangt allerdings nach einer umfassenden Aus- und ständigen Fortbildung der Ermittlungspersonen.
Ferner obliegt es dem Gesetzgeber die Maßnahmen der etwas in die Jahre gekommen StPO an die technischen Veränderungen und Weiterentwicklungen in der modernen Kommunikationstechnik anzupassen, um so Rechtsunsicherheiten und Rechtsverletzungen vorzubeugen.

Daher:
***„Reden Sie nicht so laut von Datenschutz; Sie machen sich verdächtig. Beharren Sie nicht so stur auf ihrer Privatsphäre; Sie werden sonst als Außenseiter registriert. (Aber registriert und kontrolliert werden Sie natürlich ohnehin.) Man meint es gut mit ihnen, wenn man ihr Telefon abhört, ihre Verbindungen speichert und ihren Computer durchsucht.“***[189]

[189] Prantl, Süddeutsche Zeitung vom 2.Juli 2007, Nr. 149 S.4.