Bundeskriminalamt

AGNES

Auswirkungen gesetzlicher Neuregelungen auf die Ermittlungspraxis der Strafverfolgungsbehörden

ABSCHLUSSBERICHT

KI 15 RETASAST
RECHTSTATSACHENSAMMEL- UND -AUSWERTESTELLE

KI 15 RETASAST

RECHTSTATSACHENSAMMEL- UND -AUSWERTESTELLE

Projektteam:

Dr. Susanne Graf 0611 - 55 111 27

Frank Thiede 0611 - 55 111 23

Carina Merkel 0611 - 55 111 21

Sabrina Winkler 0611 - 55 111 20

ki15@bka.bund.de

Stand: April 2008

Inhaltsverzeichnis

ABKÜRZUNGSVERZEICHNIS[1]

ABG-Räume	Arbeits-, Betriebs- und Geschäftsräume
Abs.	Absatz
a.F.	alte Fassung
AGNES	Titel des Projektes „Auswirkungen gesetzlicher Neuregelungen auf die Ermittlungspraxis der Strafverfolgungsbehörden“
Art.	Artikel
AufenthG	Gesetz über den Aufenthalt, die Erwerbstätigkeit und die Integration von Ausländern im Bundesgebiet vom 30.07.2004 (BGBl. 2004 I S. 1950) (Aufenthaltsgesetz)
Aufl.	Auflage
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHSt	Entscheidungen des Bundesgerichtshofs in Strafsachen
BKA	Bundeskriminalamt
BT-Drs.	Drucksache des Bundestags
BtMG	Betäubungsmittelgesetz in der Fassung vom 01.03.1994 (BGBl. 1994 I S. 359)
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
CR	Computer und Recht (Zeitschrift)
DPolBl	Deutsches Polizeiblatt (Zeitschrift)
Drs.	Drucksache
DuD	Datenschutz und Datensicherheit (Zeitschrift)
DVBl.	Deutsches Verwaltungsblatt (Zeitschrift)
ElAu-Dienststelle	Dienststellen, die für die technische Realisierung bei elektronischer Aufklärung zuständig sind
GA	Goltdammers Archiv für Strafrecht (Zeitschrift)
GBA	Generalbundesanwalt(-schaft)
GG	Grundgesetz für die Bundesrepublik Deutschland vom 23.05.1949 (BGBl. 1949 S. 1)
HRRS	Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht (www.hrr-strafrecht.de)
IP	Internet Protocol
JA	Juristische Arbeitsblätter (Zeitschrift)

[1] Auf die Wiedergabe allgemein üblicher Abkürzungen wurde verzichtet.

JR	Juristische Rundschau (Zeitschrift)
KOMGÜT	Kommission Grundlagen der Überwachungstechnik des UA IuK
K&R	Kommunikation und Recht (Zeitschrift)
KWKG	Gesetz über die Kontrolle von Kriegswaffen vom 20.04.1961 (BGBl. 1961 I S. 444) (Kriegswaffenkontrollgesetz)
LG	Landgericht
LKÄ	Landeskriminalämter
MEK	Mobiles Einsatzkommando
MMR	Multimedia und Recht (Zeitschrift)
NJW	Neue Juristische Wochenschrift (Zeitschrift)
NStZ	Neue Zeitschrift für Strafrecht (Zeitschrift)
NVwZ	Neue Zeitschrift für Verwaltungsrecht (Zeitschrift)
OLG	Oberlandesgericht
PC	Personal Computer
PGP	pretty good privacy
PSIS	Programm zur Stärkung der Inneren Sicherheit
Rdnr.	Randnummer
RETASAST	Rechtstatsachensammel- und -auswertestelle
SOG	Sicherheits- und Ordnungsgesetz
StGB	Strafgesetzbuch in der Fassung vom 01.01.1999 (BGBl. 1998 I 3324)
StPO	Strafprozessordnung
StraFo	Strafverteidiger Forum (Zeitschrift)
StV	Strafverteidiger
TKÜ	Telekommunikationsüberwachung
UA IuK	Unterausschusses „Informations- und Kommunikationstechnik“
VE	Verdeckter Ermittler
VoIP	Voice over Internet Protocol
VP	Vertrauensperson
WaffG	Waffengesetz in der Fassung vom 08.03.1976 (BGBl. 1976 I S. 432)
ZKA	Zollkriminalamt
ZRP	Zeitschrift für Rechtspolitik (Zeitschrift)

Vorwort

Das Projekt AGNES „Auswirkungen gesetzlicher Neuregelungen auf die Ermittlungspraxis der Strafverfolgungsbehörden“ beschäftigt sich mit drei Themenkomplexen:

- der Situation der Wohnraumüberwachung nach §§ 100c ff. StPO,
- den Schwierigkeiten der Ermittlungsbehörden bei Verfahren im Zusammenhang mit der Bildung terroristischer Vereinigungen nach § 129a Abs. 2 StGB und
- der Ermittlungspraxis im Zusammenhang mit der Nutzung moderner Kommunikationsmittel.

Die Untersuchung gibt einen Überblick darüber, wie sich die Umsetzung rechtlich komplexer und erst kürzlich neu normierter Themenbereiche in der polizeilichen Praxis gestaltet. In erster Linie wird dargelegt, welche Schwierigkeiten die Polizeien bei der Umsetzung der jeweiligen normativen Vorgaben im polizeilichen Alltag haben. Daher handelt es sich bei dem Projekt AGNES um Rechtstatsachenforschung, was die Anbindung an den Fachbereich KI 15 des BKA erklärt, dessen Aufgabe neben anderen die Sammlung und Auswertung von Rechtstatsachen ist (RETASAST).

Der Diskussion über die ausgewählten Themen kommt insbesondere eine Vernetzungsfunktion zu. Anhand der Erkenntnisse des Projekts ist es möglich, das eigene polizeiliche Handeln zu hinterfragen. Ferner können neue bzw. andere polizeipraktische Herangehensweisen anhand der Projektergebnisse erwogen werden. Darüber hinaus kann der Bericht für die rechtspolitische Diskussion hilfreich sein.

Das Projekt AGNES wurde im Oktober 2006 mit den Polizeien des Bundes und der Länder abgestimmt. Ganz offensichtlich gab und gibt es in der polizeilichen Praxis ein hohes Interesse an einem Austausch über Probleme bei den genannten Ermittlungsmaßnahmen bzw. Strafnormen und über Möglichkeiten, derartige Ermittlungen im Rahmen des geltenden Rechts effizienter zu führen. Zudem zeigte sich, dass in der Polizeipraxis konkretes Interesse hinsichtlich einer normativen Ausgestaltung der untersuchten Ermittlungsmaßnahmen bzw. Straftaten besteht.

Der große Bedarf an den Fragestellungen des Projekts führte dazu, dass die jeweiligen RETASAST-Ansprechpartner in den Ländern und im Bund sowie die mit einzelnen

Ermittlungen befassten Dienststellen, insbesondere die ElAu-Dienststellen, mit großem Engagement die Datenerhebung unterstützten und vielfach von sich aus auf praktische Probleme hinwiesen. Dabei war die Unterstützung von AGNES für die einzelnen Dienststellen mit nicht unerheblichem Aufwand verbunden. Deshalb bedankt sich das Projektteam des BKA bei allen Mitwirkenden herzlich für die große Unterstützung. Ohne diese engagierte Zuarbeit seitens der RETASAST-Ansprechpartner und der einzelnen Dienststellen wäre das Projekt nicht zu realisieren gewesen.

In diesem Abschlussbericht werden alle erlangten Erkenntnisse dargestellt und bewertet. Darüber hinaus enthält der Bericht Handlungsempfehlungen, die hinsichtlich nach wie vor rechtlich nicht eindeutig geklärter Einzelfragen Entscheidungen vor Ort erleichtern sollen. Zudem finden sich darin für die Polizeipraxis nutzbare Musterformulierungen, z.B. aus richterlichen Beschlüssen zu § 100c StPO. Damit wird den sachbearbeitenden Dienststellen die Stellung von Anträgen auf staatsanwaltschaftliche bzw. richterliche Entscheidungen erleichtert. Auch werden, so die Intention des Projekts, durch derartige Musterformulierungen rechtssichere Handlungsempfehlungen herausgegeben und argumentativ überzeugende Beschlussanregungen vereinfacht. Die in dem Bericht enthaltenen Handlungsempfehlungen dienen dazu, der polizeilichen Praxis den Umgang mit bestimmten Problemstellungen zu erleichtern. Die Empfehlungen bedeuten jedoch nicht, dass insoweit nicht gleichwohl rechtspolitischer Handlungsbedarf bestehen kann.

Ziel der Erhebung ist es ferner, vorhandene Skepsis gegenüber bestimmten Ermittlungsmaßnahmen abzubauen, die häufig aus einer Unsicherheit darüber resultiert, wie derartige Maßnahmen rechtskonform, gleichwohl aber praktikabel und Erfolg versprechend durchgeführt werden können.

Bei der Durchführung der Evaluation und der Erstellung des vorliegenden Abschlussberichts stand stets das Ziel im Vordergrund, für die polizeiliche Praxis relevante Erkenntnisse zu gewinnen und praktikable Handlungsempfehlungen zu erstellen. Wegen dieses starken Praxisbezugs erheben die Untersuchungen und dieser Bericht, was die Methodik der Erkenntnisgewinnung und die Präsentation der Ergebnisse anbelangt, nicht den Anspruch, mit rein wissenschaftlichen (empirischen bzw. rechtswissenschaftlichen) Forschungen vergleichbar zu sein.
So wurde beispielsweise im Rahmen des vorliegenden Berichts bewusst darauf verzichtet, im Zusammenhang mit den erwähnten Beschlüssen das betreffende Gericht, das Aktenzeichen und das Datum des jeweiligen Beschlusses aufzuführen, um Rückschlüsse auf

konkrete, noch nicht abgeschlossene Verfahren zu verhindern, die Ermittlungserfolge gefährden könnten.

Dieser Bericht versteht sich nicht als eine weitere theoretisch-wissenschaftliche Abhandlung zu den genannten Themenkomplexen. Er zielt darauf ab, in erster Linie der polizeilichen Praxis und daneben auch der Rechtspolitik konkrete Hinweise und Empfehlungen zu geben. Deshalb wurde auch davon abgesehen, die wissenschaftliche Diskussion im Einzelnen nachzuzeichnen. Die zu den jeweiligen Themen veröffentlichte Literatur wurde jedoch vollständig ausgewertet. Da sich das Projekt in erster Linie an Praktiker in der Sachbearbeitung richtet, wurden technische Details oftmals nur grob umrissen.

Im Anhang ist eine Auswahlbibliographie enthalten, die thematisch geordnet auf weiterführende Literatur zu den einzelnen Problembereichen hinweist.

Das Projektteam

I. AUSGANGSSITUATION UND VORGEHENSWEISE

1. Hintergrund

Das Projekt AGNES ist im Rahmen der RETASAST, also des Aufgabenfeldes der Sammlung und Auswertung von Rechtstatsachen im Fachbereich KI 15 im BKA, konzipiert und realisiert worden. Wie bei der RETASAST selbst geht es bei dem Projekt um Rechtstatsachenforschung anhand von Erkenntnissen aus der polizeilichen Praxis und für die polizeiliche Praxis.

Bei Auswahl der Themen des Projekts AGNES wurde maßgeblich berücksichtigt, auf welche Problemstellungen sich die Anfragen an die RETASAST häufig bezogen. Dies ist auch der Grund dafür, dass einige der untersuchten Aspekte schon in die halbjährlich erscheinende Bund-Länder-Fallsammlung[2] eingeflossen sind.

Rechtstatsachen können auch einen wichtigen Beitrag leisten, um Rechtssetzungsbedarf aufzuzeigen Insofern stellt die Rechtstatsachensammlung, an die dieses Projekt angebunden ist, ein wesentliches Instrument der Rechtspolitik dar.

Ziel des Projektes ist jedoch neben dem Aufzeigen von fachlichem Rechtssetzungs- oder Rechtsänderungsbedarf primär die Darstellung der nach geltender Rechtslage erkannten Problempunkte aus Sicht der polizeilichen Praxis und ihr Umgang mit den gesetzlichen Vorgaben in den ausgewählten Themenfeldern.

[2] Die Bund-Länder-Fallsammlung ist in Extrapol zu finden unter Startseite > Bildung & Wissen > Literatur & Recherche > Infostellen > RETASAST > Bund-Länder-Fallsammlung.

2. Projektmethodik

Das Projekt AGNES wurde von Oktober 2006 bis März 2008 durchgeführt.

In einer **ersten Stufe** des Projekts wurde anhand einer Bund-Länder-Befragung ermittelt, hinsichtlich welcher Themenbereiche ein vordringlicher Evaluierungsbedarf bestand. Anschließend wurden die zu bearbeitenden Themen festgelegt.

Im Rahmen der darauf folgenden **zweiten Stufe**, die im Februar 2007 endete, wurde zunächst ein standardisierter **Fragebogen** zu jedem Projektthema erstellt. Dieser Fragebogen wurde anschließend vom BKA, Fachbereich KI 15-RETASAST, in Abstimmung mit den Polizeien der Länder, der Bundespolizei und dem ZKA sowie in Kooperation mit den ermittlungsführenden Bereichen im BKA entworfen.[3]

Von Februar bis August 2007 wurde mittels der Fragebögen eine Erhebung bei allen Polizeien der Länder und des Bundes durchgeführt. Diese Befragung bezog sich nicht nur auf aktuelle Verfahren, sondern auch auf zurückliegende Fälle.

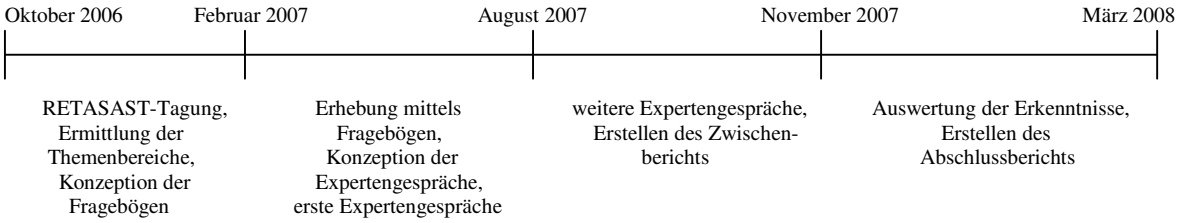
Die Dienststellen wurden ersucht, für jede erfolgte Ermittlungsmaßnahme einen Fragebogen auszufüllen und auch dann eine Rückmeldung zu geben, wenn eine Maßnahme „nur“ angedacht, aber aus näher auszuführenden Gründen nicht gegenüber der Staatsanwaltschaft oder dem zuständigen Gericht angeregt, nicht beantragt oder zwar beantragt, aber durch die Staatsanwaltschaft oder das Gericht abgelehnt worden war.

In einer **dritten Stufe** des Projekts wurden ab Juli 2007 vertiefende **Expertengespräche** mit den betroffenen Polizeidienststellen geführt. In den Expertengesprächen wurde nach persönlichen Erfahrungen, Vorstellungen und Verbesserungsvorschlägen gefragt. Darüber hinaus konnten im Detail persönliche Erfahrungen und Einschätzungen der unmittelbar in einzelne Maßnahmen involvierten Sachbearbeiter erfasst werden. Insbesondere konnte so die aus der praktischen Anwendung der betrachteten Normen resultierende Kritik aufgenommen werden. Ferner haben die Expertengespräche dazu gedient, die Erkenntnisse, die aus den Fragebögen erlangt wurden, zu überprüfen sowie zu vertiefen.

Außerdem hatten Mitglieder des Projektteams Gelegenheit, an Treffen verschiedener Gremien, auf denen z.B. aktuelle Probleme der Wohnraumüberwachung diskutiert wurden,

teilzunehmen. Zudem nahmen Projektteammitglieder beobachtend an einer Hauptverhandlung wegen Mitgliedschaft in einer terroristischen Vereinigung gemäß § 129a StGB teil.

In der **vierten** und letzten **Stufe** wurden von Dezember 2007 bis Februar 2008 alle Erkenntnisse, die im Rahmen der bisherigen Projektarbeit gewonnen worden waren, ausgewertet sowie für diesen **Abschlussbericht** zusammengetragen und bewertet.



[3] Die erstellten Erhebungsbögen sind im Anhang zu diesem Bericht abgedruckt.

II. AUSWERTUNG

Die Zahl der Zulieferungen durch die Polizeien der Länder, die Bundespolizei, das ZKA und das BKA war je nach Themenkomplex sehr unterschiedlich.

Bezüglich des **Themenkomplexes Wohnraumüberwachung** wurden mit den insgesamt 16 zurückgesandten Erhebungsbögen alle Verfahren erfasst, die in Deutschland seit dem Urteil des BVerfG zur akustischen Wohnraumüberwachung durchgeführt wurden. Eine Ausnahme bildeten zwei Verfahren, zu denen weder die Verfahrensakten ausfindig gemacht noch die damals mit den Verfahren befassten Sachbearbeiter ermittelt werden konnten. Hinsichtlich dieses Themenkomplexes wurde also annähernd eine Vollerhebung erreicht.

Im Rahmen des **zweiten Themenkomplexes** wurden sämtliche polizeilichen Stellen kontaktiert, die **Ermittlungen wegen des Verdachts der Bildung einer terroristischen Vereinigung** führen bzw. geführt haben. Die in Deutschland seit der Novellierung des § 129a Abs. 2 StGB im Jahr 2003 zu diesem Themenbereich durchgeführten Verfahren konnten daher vollständig erfasst werden. Dies gilt sowohl für die Verfahren, die vom BKA geführt wurden, als auch für die von den Ländern betriebenen Ermittlungen. Es handelt sich auch insofern um eine Vollerhebung.

Dagegen waren der Rücklauf von Erhebungsbögen zum **dritten Themenkomplex**, der **Ermittlungspraxis im Zusammenhang mit der Nutzung moderner Kommunikationsmittel**, sowie die Erkenntnisse aus den hierzu durchgeführten Expertengesprächen gering. Ursächlich hierfür könnte die große Unsicherheit innerhalb der Dienststellen bei der Durchführung von Maßnahmen im Zusammenhang mit der Nutzung moderner Kommunikationsmittel sein. So wurde beispielsweise hinsichtlich der Online-Durchsuchung danach gefragt, in welchen Fällen eine solche Maßnahme angedacht worden war. Durch die Entscheidung des BVerfG vom 27.02.08 wurde klargestellt, dass die Schaffung einer Befugnisnorm zur Online-Durchsuchung auch in der StPO nach Maßgabe der Vorgaben des Senats jedenfalls verfassungsrechtlich möglich ist.
Die geltende Rechtslage lässt eine Online-Durchsuchung seit der Entscheidung des BGH vom 31.01.07 nicht zu. Da dies den Polizeidienststellen und Staatsanwaltschaften bekannt ist, sind auch im Erhebungszeitraum jedenfalls nach dem 31.01.07 Anregungen an die StA oder Anträge bei den Ermittlungsrichtern nicht zu verzeichnen. Daher ist der geringe zahlenmäßige Rücklauf zu diesem Thema nachvollziehbar.

1. Themenkomplex: Akustische Wohnraumüberwachung gemäß §§ 100c ff. StPO

Unter einer Wohnraumüberwachung wird die akustische Erfassung und Aufzeichnung von Gesprächen und anderen Äußerungen, einschließlich Geräuschen, verstanden, die innerhalb von Wohnungen geführt bzw. getätigt werden. Solche Maßnahmen haben besondere Brisanz, da sie in den Schutzbereich des Art. 13 Abs. 1 GG (Unverletzlichkeit der Wohnung) eingreifen, der den Einzelnen grundsätzlich davor bewahrt, dass sein Verhalten innerhalb typischer persönlicher Rückzugsräume durch staatliche Maßnahmen bekannt wird. Akustische Wohnraumüberwachungen stellen also stets einen erheblichen Grundrechtseingriff dar.

Vor diesem Hintergrund hat das BVerfG in einer Entscheidung[4] vom März 2004 für Maßnahmen akustischer Wohnraumüberwachung sehr enge Grenzen gezogen. Ein wesentlicher Aspekt dieser Entscheidung ist das Erfordernis des Schutzes des Kernbereichs privater Lebensgestaltung. Der Gesetzgeber hat durch die Novellierung der §§ 100c ff. StPO vom 24.06.2005[5] die akustische Wohnraumüberwachung innerhalb des vom BVerfG gezogenen Rahmens neu geregelt, so dass sie einerseits den vom BVerfG postulierten Anforderungen an den Schutz des Kernbereichs privater Lebensgestaltung genügt, andererseits aber auch als Ermittlungsinstrument erhalten bleibt.

Eine erneute Verfassungsbeschwerde gegen den novellierten § 100c StPO hat das BVerfG mit Kammerbeschluss[6] vom 11.05.2007 mangels Aussicht auf Erfolg gar nicht erst zur Entscheidung angenommen. Die neu gefasste Regelung der akustischen Wohnraum-überwachung werde den grundgesetzlichen Anforderungen an die Rechtmäßigkeit eines Eingriffs in die räumliche Privatsphäre gerecht. Insbesondere sei die so genannte negative Kernbereichsprognose ausreichend, bei der tatsächliche Anhaltspunkte dafür vorliegen müssen, dass durch die Maßnahme voraussichtlich nicht in den Kernbereich privater Lebensgestaltung eingegriffen wird.

[4] Vgl. BVerfGE 109, 279 ff.
[5] Vgl. BGBl. 2005 I S. 1841.
[6] Vgl. BvR 543/06.

In der polizeilichen Praxis bestanden und bestehen jedoch ganz erhebliche Bedenken, ob im Rahmen dieser neuen normativen Vorgaben akustische Wohnraumüberwachungen überhaupt noch Erfolg versprechend durchgeführt werden können.
Dies gilt unabhängig davon, dass akustische Wohnraumüberwachungen auch schon vor der Entscheidung des BVerfG nur als ultima ratio-Maßnahme durchgeführt wurden. Während die geringe Zahl der durchgeführten akustischen Wohnraumüberwachungen einerseits zeigt, dass den Erfordernissen eines effektiven Grundrechtsschutzes Rechnung getragen wird, so bedeutet dies andererseits zugleich, dass möglicherweise Erfolg versprechende letzte Ermittlungsansätze in der Praxis ungenutzt bleiben.

Die Evaluation von Wohnraumüberwachungsmaßnahmen im Rahmen des Projekts AGNES dient der Feststellung, worauf der Rückgang solcher Maßnahmen beruht und wie die Umsetzung der vom BVerfG aufgestellten Anforderungen an den Schutz des Kernbereichs persönlicher Lebensgestaltung in der Polizeipraxis gelingt.

Für den vorliegenden Bericht wurden 16 Fragebögen[7] sowie 15 Expertengespräche ausgewertet. Zu drei aktuellen Maßnahmen liegen keine Erhebungsbögen vor, da es sich um laufende Ermittlungsverfahren handelt, die noch keiner abschließenden Bewertung durch die jeweilige Dienststelle unterlagen. Diese Maßnahmen wurden jedoch im Rahmen von Expertengesprächen in die Auswertung einbezogen. Auf diesem Weg sind auch die zu diesen Maßnahmen erlangten Erkenntnisse in den Abschlussbericht eingeflossen. Im Folgenden werden die gewonnenen zentralen Erkenntnisse dargestellt.

1.1. Entwicklung der Wohnraumüberwachung seit dem Urteil des BVerfG

Seit dem Urteil des Bundesverfassungsgerichts zur Wohnraumüberwachung macht die polizeiliche Praxis von diesem Ermittlungsinstrument nur noch sehr zurückhaltend Gebrauch.

Anzahl der Wohnraumüberwachungsmaßnahmen

Jahr	Zahlen aus Statistik der Bundesregierung	Zahlen aus der Erhebung im Projekt AGNES
2003	37	*
2004	11	3*
2005	7	5
2006	2	3
2007	noch nicht veröffentlicht	7**

[7] Drei davon betrafen Ermittlungen nach § 100c Abs. 1 Nr. 1 StPO aF..

* Im Rahmen des Projekts wurden Maßnahmen nach § 100c StPO ab März 2004 erhoben.
** Drei der Maßnahmen im Jahr 2007 betreffen laufende Ermittlungsverfahren, zu denen nur Expertengespräche geführt wurden. Da die Erhebung im Oktober 2007 endete, sind nicht zwingend alle Maßnahmen aus dem Jahr 2007 erfasst.

Während ausweislich der jährlichen Berichte der Bundesregierung[8] gemäß Art. 13 Abs. 6 Satz 1 GG i.V.m. § 100e Abs. 1 StPO im Jahr 2003 noch 37 Wohnraumüberwachungsmaßnahmen angeordnet wurden, waren es 2004 nur noch elf und 2005 nur noch sieben, wobei lediglich sechs dieser sieben Maßnahmen tatsächlich realisiert wurden. 2006 wurden sogar nur noch zwei Maßnahmen angeordnet und durchgeführt.

Die Abweichungen der Zahlen aus der Statistik der Bundesregierung und der AGNES-Erhebung ergeben sich für das Jahr 2004 schlicht daraus, dass mit dem Projekt erst die Maßnahmen nach dem Urteil des BVerfG gezählt wurden.
Nach der im Rahmen des Projekts AGNES durchgeführten Erhebung hat es jedoch auch im Berichtsjahr 2005 zwei angeordnete Wohnraumüberwachungen weniger gegeben als nach der Statistik der Bundesregierung. Diese Diskrepanz wurde seitens der Länder in einem Fall mit einer Mehrfachzählung einer Maßnahme in der Statistik der Bundesregierung erklärt, da ein Verfahren unter verschiedenen Aktenzeichen geführt worden sei. In dem anderen Fall handelte es sich um ein länderübergreifendes Verfahren, welches gleichfalls zu einer Mehrfachnennung der Maßnahme führte. Zwei weitere in der Statistik der Bundesregierung aufgeführte Verfahren konnten nicht in diesen Abschlussbericht einbezogen werden, da zu beiden Maßnahmen keine Unterlagen sowie Auskunftspersonen mehr ermittelbar waren.
Für 2006 wurden dagegen drei statt der zwei in der Bundesstatistik gezählten Verfahren gemeldet.

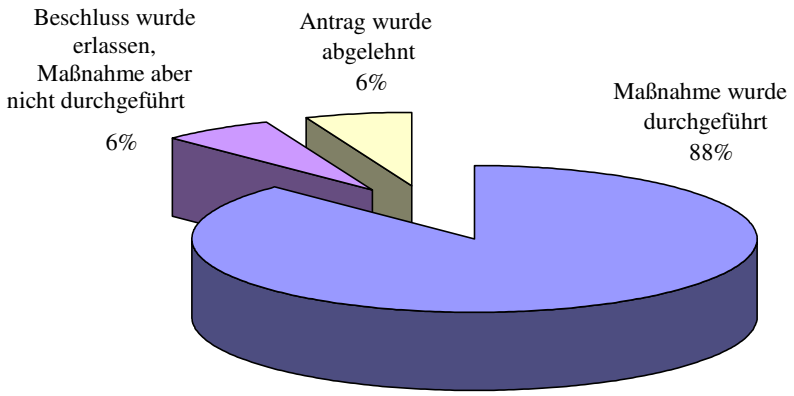
Eine Doppelzählung von nach § 100c StPO durchgeführten Maßnahmen in der Statistik der Bundesregierung ließe sich vermeiden, wenn sich die Daten erhebende Stelle jeweils anonymisierte Abschriften der nach § 100c StPO erlassenen Beschlüsse durch die betroffenen Organisationseinheiten vorlegen ließe. Dadurch könnten sowohl Verfahren, die unter verschiedenen Aktenzeichen geführt werden, als auch länderübergreifende Verfahren als jeweils ein Verfahren erfasst werden, wobei letztgenannte Verfahren dann für das Land zu zählen wären, in dem der betreffende Beschluss erlassen wurde.

[8] Vgl. BT-Drs. 15/3699 für 2003; 15/5971 für 2004; 16/3068 für 2005; 16/6363 für 2006.

Wurde die Wohnraumüberwachungsmaßnahme durchgeführt?

	Häufigkeit	Prozent
Antrag abgelehnt	1	6 %
Maßnahme nicht durchgeführt	1	6 %
Maßnahme durchgeführt	14	88 %
Gesamt	**16**	**100 %**

Insgesamt wurden nach den Erkenntnissen des Projekts von März 2004 bis Oktober 2007 **15 Maßnahmen** nach § 100c StPO gerichtlich **angeordnet**. Eine dieser Maßnahmen wurde jedoch nicht realisiert, da der Einbau der Technik nicht gelang, weil nicht ohne Enttarnung der Maßnahme in das zu überwachende Objekt gelangt werden konnte. Eine weitere Maßnahme wurde zwar beantragt, doch hat das zuständige Gericht den Erlass eines Beschlusses wegen unzureichenden Tatverdachts abgelehnt.



1.2. Objekte, die von Maßnahmen nach § 100c StPO betroffen waren

Die möglichen Örtlichkeiten, in denen Maßnahmen nach § 100c StPO durchgeführt werden dürfen, lassen sich nach der Rechtsprechung in drei verschiedene Kategorien einteilen, wobei alle Räumlichkeiten von Art. 13 GG geschützt sind, aber unter Umständen eine abgestufte Schutzwürdigkeit aufweisen:

- Als **Privatwohnungen** sind alle abgegrenzten Räume anzusehen, die der allgemeinen Zugänglichkeit durch eine räumliche Abschottung entzogen und zur Stätte privaten Lebens und Wirkens gemacht worden sind,[9] z.B. Wohnräume jeder Art, auch Zweitwohnungen, Untermietwohnungen, Wochenendhäuser, Miethäuser, Altersheime, Studentenwohnheime, einschließlich Nebenräumen wie Böden, aber auch Hausboote, Zelte sowie Krankenzimmer[10]. Alle Zubehörflächen, die in erkennbarem Zusammenhang mit Wohnraum stehen, wie Keller, Hof oder Garten[11], sind ebenfalls vom Wohnungsschutz umfasst.
- **Arbeits-, Betriebs- und Geschäftsräume** (ABG-Räume) sind Räume, die grundsätzlich der Öffentlichkeit zugänglich sind, aber in den Zeitspannen, in denen sie gerade nicht öffentlich zugänglich sind, als schutzwürdig erachtet werden. Beispielsweise sind das Läden, Kanzlei- und Praxisräume, Büroräume[12], Verkaufsräume, Gaststätten, Imbissräume, Werkstätten, Montagehallen, Scheunen, Stallungen oder Lagerhallen.
- **Sonstige geschützte Räume** sind z.B. Kirchen und Klöster, abgeschlossene Höfe, Schlafwagenabteile, Hotelzimmer, Vereinshäuser oder Clubräume.

In einzelnen, gerichtlich noch nicht geklärten Fällen ist die Frage, ob eine der gerade aufgeführten Kategorien vorliegt oder ein Objekt betroffen ist, welches nicht unter den Wohnungsbegriff subsumiert wird (und damit Überwachungsmaßnahmen nach **§ 100f StPO** möglich sind) von den Strafverfolgungsbehörden bzw. den Staatsanwaltschaften unterschiedlich gehandhabt worden. Beispielhaft seien folgende Fälle genannt:

- Die akustische Überwachung eines **Campingbusses** erachteten zwei Staatsanwaltschaften als Eingriff in Art. 13 GG. Aufgrund dessen wurde ein Kernbereichsschutz durch eventuelles Abschalten des Aufnahmegerätes gefordert.

[9] Vgl. BGHSt 42, 372.
[10] Vgl. BGHSt 50, 206 (211 f.), jedenfalls dann, wenn der Patient nicht dauernder Überwachung bedarf.
[11] Vgl. BGH NJW 1997, 196.

Ein Differenzierungsvorschlag dahingehend, das Fahrzeug während der Fahrt nicht als Wohnung anzusehen, sondern nur das stehende und als „Wohnwagen“ genutzte Fahrzeug als Wohnung einzustufen, lehnte man ab.

- Die Überwachung einer **Lkw-Fahrerkabine** stufte die Mehrheit der angehörten Experten als Wohnraumüberwachungsmaßnahme ein, sofern eine Schlaf- und Kochgelegenheit vorhanden ist.
- In einem weiteren Fall wurde die Überwachung eines **Büroraumes während der Geschäftszeiten** nach § 100f StPO realisiert, obwohl der Raum eine abgeschottete Lage aufwies und lediglich für einen eng begrenzten Personenkreis zugänglich war.
- Die Überwachung eines **Bauwagen-Containers** auf dem Gelände eines Gebrauchtwagenhandels wurde von einem Gericht als Wohnraumüberwachungsmaßnahme eingestuft. Der Fall wurde zwar nach alter Rechtslage beurteilt, dies ist aber hinsichtlich der hier erörterten Differenzierung „innerhalb – außerhalb Wohnraum“ ohne Relevanz.

Im Übrigen ist durch die Rechtsprechung geklärt, dass folgende Räume **keinen Wohnraum** im Sinne des § 100c StPO darstellen:

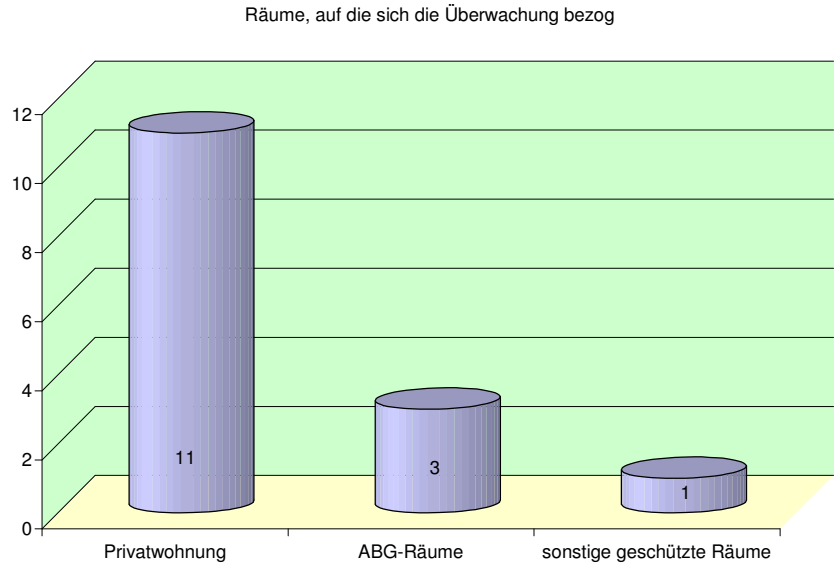
- Besucherräume in Untersuchungsgefängnissen[13],
- eine Haftzelle[14],
- Unterkunftsräume für Soldaten oder Polizeibeamte[15] sowie
- ein Pkw[16].

Art der Räume, auf welche sich die Wohnraumüberwachung bezog

	Häufigkeit	Prozent
Privatwohnung	11	73 %
ABG-Raum	3	20 %
sonstiger geschützter Raum	1	7 %
Gesamt	**15**	**100 %**
Fehlend (kein Beschluss erlassen)	**1**	

[12] Vgl. BGHSt 42, 372 sowie OLG Stuttgart StV 1996, 655 f. für Räume der PKK.
[13] Vgl. BGHSt 50, 211.
[14] Gleichwohl schließt die Achtung der Menschenwürde des Gefangenen die Pflicht ein, die Privat- und Intimsphäre als Ausdruck des allgemeinen Persönlichkeitsrechts aus Art. 1 Abs. 1, Art. 2 Abs. 1 GG zu wahren, vgl. BVerfG NJW 1996, 2643.
[15] Vgl. BGH NStZ 1999, 46.
[16] Vgl. LG Stendal NStZ 1994, 556.

Räumlich fanden die untersuchten Maßnahmen nach § 100c StPO **überwiegend** – bei elf von 15 Beschlüssen nach § 100c StPO – in **Privatwohnungen** statt; in einem Verfahren wurde der Erlass eines § 100c StPO-Beschlusses abgelehnt. Bezüglich der zweiten Kategorie, den **ABG-Räumen**, wurde je eine Maßnahme in einem Friseursalon, dem Nebenraum einer Kantine sowie einem TÜV-Prüfungsraum durchgeführt bzw. angedacht. Eine Maßnahme fand in einem **sonstigen geschützten Raum**, dem Getränkelager einer Gaststätte statt. Dagegen ist die Überwachung eines Hotelzimmers vom zuständigen Gericht mangels hinreichenden Tatverdachts (und nicht wegen der Örtlichkeit) abgelehnt worden.



Als **Inhaber der Räume** ist der jeweilige unmittelbare Besitzer anzusehen, also z.B. der Mieter, Untermieter, Gast im Hotel, Mitbesitzer (z.B. bei einer Lebensgemeinschaft), der Besitzdiener (z.B. Internatsschüler, Obdachlose im Obdachlosenheim, Patienten im Krankenzimmer) oder bei Geschäftsräumen der Unternehmer, nicht dagegen der Vermieter oder Eigentümer.

Die Auswertung der Fragebögen ergab, dass die Beschuldigten in zehn Fällen Inhaber der betroffenen Räumlichkeiten waren, in fünf Fällen Dritte, von denen zwei ihr Einverständnis zu der Wohnraumüberwachung erteilt hatten.

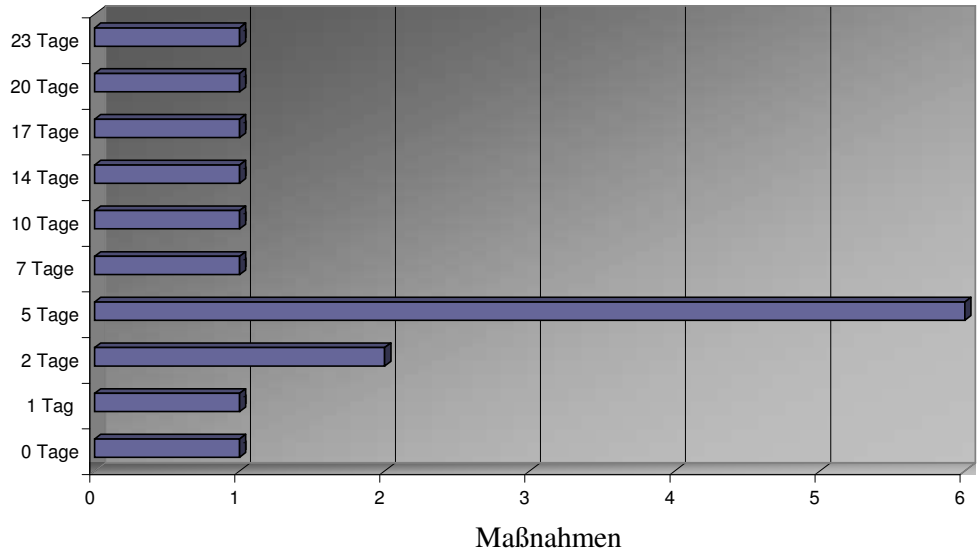
1.3. Vorbereitende Ermittlungsschritte

Die **Gründe für die Planung bzw. Durchführung einer Wohnraumüberwachung** waren in den betrachteten Fällen sehr unterschiedlich. In acht Fällen bestand aufgrund tatsächlicher Anhaltspunkte der Verdacht, dass in dem zu überwachenden Objekt Straftaten verabredet bzw. abgewickelt wurden. In zwei Fällen waren andere operative Maßnahmen aufgrund der hohen Konspirativität der Beschuldigten nicht Erfolg versprechend. Ähnlich gelagert war ein Fall, in dem die beiden Beschuldigten, ein Ehepaar, aufgrund ihrer gemeinsamen Lebensführung nur in der Wohnung miteinander kommunizierten.

In den durchgeführten Expertengesprächen wurden mehrheitlich als **Vorbereitungszeit** für eine Maßnahme nach § 100c StPO je nach Objekt und Situation zwischen sieben Tagen und vier Wochen angegeben. Teilweise dauerte die Vorbereitung, innerhalb derer dann allerdings parallel andere Maßnahmen ergriffen wurden, deutlich länger, im Einzelfall bis zu sechs Monaten.

Vorbereitungsdauer

(in Tagen)	Häufigkeit	Prozent
0	1	6,25 %
1	1	6,25 %
2	2	12,5 %
5	6	37,5 %
7	1	6,25 %
10	1	6,25 %
14	1	6,25 %
17	1	6,25 %
20	1	6,25 %
23	1	6,25 %
Gesamt	**16**	**100 %**



Die Angaben in den Expertengesprächen weichen hier zum Teil deutlich von den Antworten in den Fragebögen ab. In Letzteren wurde für die überwiegende Anzahl der Fälle eine Vorbereitungszeit von bis zu zehn Tagen angegeben, nur in vier Fällen wurden Zeiten zwischen zwei und vier Wochen genannt.

Festzuhalten bleibt jedoch als Ergebnis der Auswertung sowohl der Fragebögen als auch der Expertengespräche, dass die erforderliche Vorbereitungszeit **nicht zu unterschätzen** ist und in der Regel ein oder zwei Tage nicht ausreichen dürften. Eine zu kurze Vorbereitung, beispielsweise bei Ad-hoc-Maßnahmen, begründet die Gefahr, dass die Maßnahme scheitert. Die Gründe für ein solches Scheitern können vielseitig sein. Sie reichen von einer Ablehnung des beantragten Beschlusses, da keine ausreichende Prognose hinsichtlich der Wahrung des Kernbereichs möglich ist, über technische Schwierigkeiten bei der Maßnahmenrealisierung bis hin zu einem unvertretbar hohen Entdeckungsrisiko.

Dies schließt andererseits nicht aus, dass es gleichwohl in einzelnen Konstellationen (Eilfälle) gibt, in denen eine kurzfristige Anordnung und Durchführung der Maßnahme erforderlich ist, z.B. aufgrund von bereits vorhandenen Vorerkenntnissen über das Objekt, die Zielpersonen sowie prognoserelevanter Kernbereichserkenntnisse.

Für die optimale Realisierung einer Wohnraumüberwachung ist vor allem eine frühzeitige Einbindung der operativen ElAu-Dienststelle/des MEK erforderlich.

Als problematisch wurde von den befragten Experten angesehen, dass bereits zur Vorbereitung einer Maßnahme nach § 100c StPO ein **Betreten des jeweiligen Objekts** und hierfür ein **zeitlich befristeter richterlicher Beschluss erforderlich** ist. Taktische Probleme hätten sich dabei – so die Experten – im Zusammenhang mit dem verdeckten Betreten der betroffenen Wohnung sowie dem Öffnen gesicherter Türen ergeben.

Dass neben dem Betreten zur Anbringung auch das Entfernen der Technik von der Anordnung umfasst ist, kann zwecks Rechtssicherheit für die eingesetzten Beamten in der richterlichen Anordnung klargestellt werden, wie es z.B. in den folgenden Beschlüssen formuliert wurde:

> *„Das Betreten des Objektes zum Anbringen und Entfernen der erforderlichen technischen Mittel sowie das Anbringen und Entfernen dieser Mittel zum Zwecke des Abhörens und Aufzeichnens des nichtöffentlich gesprochenen Wortes wird genehmigt."*

oder:

> *„Der Ermittlungsbehörde wird das mehrfache Betreten der zu der vorgenannten Wohnung gehörenden Räume während und nach Abschluss der Maßnahme gestattet, um die für deren Durchführung erforderlichen logistischen Voraussetzungen zu schaffen und die installierten technischen Mittel nach Beendigung wieder zu entfernen."*

Die mit der Maßnahme notwendigerweise verbundenen Vorbereitungshandlungen sind allerdings auch ohne explizite Erwähnung im richterlichen Beschluss von der Anordnung der Wohnraumüberwachung umfasst.[17]

Eine spezielle und ausführliche Darstellung im Beschluss, dass Maßnahmen zum Ein- und Ausbau der Technik zulässig sind, ist nicht zwingend erforderlich, da § 100c StPO alle erforderlichen Maßnahmen umfasst. Sie dient aber der Klarstellung und sollte angeregt werden.

Durch die Gesetzesnovelle sind die **Anforderungen, welche an vorbereitende Maßnahmen** gestellt werden, **erhöht** worden. Denn die Vorbereitung einer Wohnraumüberwachung darf sich nicht mehr darauf beschränken, die erforderliche Technik zu installieren. Vielmehr muss auch eine Prognose darüber erstellt werden, ob bzw. inwieweit eine Überwachungsmaßnahme den Kernbereich persönlicher Lebensgestaltung[18] tangiert. Das heißt, es muss dargelegt werden, wie wahrscheinlich es sein wird, dass höchstpersönliche Äußerungen erfasst und aufgezeichnet werden. Die Erforderlichkeit der Prognose ergibt sich aus dem Umstand, dass von einer Wohnraumüberwachung abzusehen ist, wenn eine Kernbereichsverletzung als wahrscheinlich gilt. Es muss aber zumindest sichergestellt sein, dass Kernbereichsrelevantes weder erfasst noch aufgezeichnet wird. Hierzu ist oftmals erforderlich, zu erkennen, ob Personen, die das Objekt betreten bzw. verlassen, einem tendenziell geschützten Personenkreis angehören.

Im Rahmen der Vorabklärung ist es in der Regel geboten, durch geeignete Maßnahmen die Lage bzw. den Charakter der Wohnung, (Privatwohnung oder Geschäftsraum), Zugangsmöglichkeiten zum Objekt sowie Erkenntnisse zu den Bewohnern des Objektes zu ermitteln. Als **zentrale flankierende Vorbereitungsmaßnahmen** sind daher unmittelbare sowie technische Observationen des Objektes zu nennen. Zudem sind diese Maßnahmen in der Regel auch während der Wohnraumüberwachung zur ständigen Prüfung der Kernbereichsrelevanz erforderlich, jedoch können hierdurch auch schon vor der Durchführung der Maßnahme Indizien für die Prognosestellung gewonnen werden.

Videoüberwachung von außen, die von den befragten Experten für in der Regel unbedingt erforderlich erachtet wird, scheitert – ungeachtet der Frage, ob insoweit im Einzelfall bereits der Schutzbereich des Art. 13 GG tangiert sein kann und die Maßnahme vor diesem Hintergrund rechtlich zulässig wäre – häufig bereits an der technisch schwierigen Realisierbarkeit, dabei hängt der Erfolg stark von externen Faktoren, wie z.B. den Lichtverhältnissen ab. Ein Erkennen von Personen kann ggf. nur an groben Äußerlichkeiten wie beispielsweise dem Haarschnitt, dem Gang oder der Statur möglich sein. Als weiteres Problem wurde geschildert, dass die Installation der Videotechnik je nach Objektlage so auffällig war, dass die gesamte verdeckte Maßnahme enttarnt zu werden drohte.

[17] Vgl. *Meyer-Goßner*, StPO, 50. Aufl. 2007, § 100c Rdnr. 7.
[18] Vgl .dazu unter 1.7.1.

Die im Rahmen des Projekts berichteten Probleme lassen sich jedoch schwer verallgemeinern, da die Aussagen sehr stark von der Lage der konkreten Wohnung und den weiteren Umständen des Einzelfalls abhängig sind.

Eine nach derzeitiger Rechtslage unzulässige repressive **Videoüberwachung im Objekt** wäre nach Ansicht der Experten sowohl zur Erstellung einer Prognose hinsichtlich der Kernbereichsbetroffenheit als auch für das rechtzeitige Erkennen einer Kernbereichsberührung hilfreich und könnte darüber hinaus sehr wahrscheinlich Stimmgutachten zur Unterscheidung der Personen, deren Äußerungen erfasst wurden, entbehrlich machen. Zudem ist bei bestimmten Fremdsprachen die Gestik bzw. Mimik bei der Aussprache entscheidend für das Sprachverständnis und eine rein akustische Überwachung für die Sinnerfassung bei mehrdeutigen Wörtern häufig ungenügend.

Beispielsweise wäre in einer der im Projekt erfassten Wohnraumüberwachungsmaßnahmen eine visuelle Überwachung der Räumlichkeiten bei Nichtkommunikation oder unverständlicher Kommunikation (insbesondere bei Fremdsprachen oder Kommunikation mehrere Personen) für die Zuordnung der Sprache bzw. zur Kompensation fehlender Erkenntnisse über das genaue Geschehen in der Wohnung erforderlich gewesen.
Im betreffenden Fall wurde die akustische Wohnraumüberwachung in einer Räumlichkeit durchgeführt, in der die Täter den Sprengstoff vorbereiten wollten. Aufgrund der schwer verständlichen Kommunikation war das Geschehen zeitweise unklar. Erschwerend kam hinzu, dass die akustische Überwachung während dieser Phase zum Schutz des Kernbereichs unmittelbar vor dem geplanten Zugriff abgeschaltet werden musste, da für die auswertenden Beamten nicht herauszuhören war, ob alle oder nur ein Täter sich in ihrem grundrechtlich abgedeckten Kernbereich der privaten Lebensführung bewegten.
Gleichwohl wird jedoch anerkannt, dass die repressive Videoüberwachung innerhalb von Objekten eine ungleich eingriffsintensivere Maßnahme darstellt und aufgrund der verfassungsrechtlichen Vorgaben nicht umzusetzen ist.

Eine weniger eingriffsintensive Maßnahme als die Videografie im Objekt wäre die – derzeit allerdings ebenfalls unzulässige – repressive **Videoüberwachung im Nahbereich von Wohnungen** im engeren Sinne, z.B. im Hausflur eines Mehrfamilienhauses[19], mithin Bereichen, die zwar nach ständiger Rechtsprechung dem Schutzbereich des Art. 13 GG unterfallen, jedoch weniger schützenswert erscheinen, als z.B. eine Privatwohnung i.e.S..

[19] Vgl. BGH NJW 1991, 2651: Eine Videoüberwachung im Treppenhaus gegenüber einer Wohnungstür tangiert Art. 13 GG.

Solche Maßnahmen im Nahbereich von Wohnungen i.e.S. könnten auch im Zusammenhang mit anderen flankierenden Maßnahmen zumindest eine Identifizierung der im Objekt Anwesenden erleichtern und ein zeitlich schnelleres Wiederzuschalten nach einer Unterbrechung aus Gründen des Kernbereichsschutzes bzw. einer Unterbrechung aufgrund richterlicher Vorgaben aus dem Beschluss ermöglichen.

Im Rahmen der Vorbereitung von Wohnraumüberwachungsmaßnahmen kommt es, wie in mehreren Expertengesprächen thematisiert, auch bei der **Mitwirkung Dritter** zu Problemen. So forderte in einem Verfahren ein Telekommunikationsdienstleister einen Beschluss nach § 100a StPO, um die Ausleitung der akustischen Signale aus der Wohnung über die Telefonleitung zu realisieren. Richtigerweise aber ermächtigen Beschlüsse nach § 100c StPO die Ermittlungsbehörden dazu, sämtliche Maßnahmen zu ergreifen, die zur Realisierung einer Wohnraumüberwachung erforderlich sind; weiterer gesonderter Beschlüsse bedarf es insofern nicht.[20]

Dabei besteht jedoch gerade keine gesetzliche Verpflichtung Dritter zur Mitwirkung bei der Realisierung der Wohnraumüberwachung. Im beschriebenen Fall musste daher eine TKÜ-Anordnung erwirkt werden, um den Dritten (hier: Betreiber) zur Unterstützungsleistung für eine Wohnraumüberwachungsmaßnahme verpflichten zu können.
Für andere Dritte, also Personen oder Unternehmen, besteht eine solche gesetzliche Verpflichtung gar nicht. In der Regel verlangen „private Dritte“, die im Einzelfall zur erfolgreichen Durchführung der Maßnahme erforderlich sind und die auf freiwilliger Basis unterstützen, wie beispielsweise Schlüsselhersteller, dass ihnen eine Ausfertigung des Beschlusses vorgelegt wird. Von Seiten der Sachbearbeitung wurde darauf hingewiesen, dass erhebliche Bedenken dagegen bestehen, generell frühzeitig Dritte durch Aushändigung eines vollständigen Beschlusses über beabsichtigte Maßnahmen in Kenntnis zu setzen.

[20] Vgl. Seite 29.

Da es keine gesetzliche Verpflichtung zur Mitwirkung Dritter gibt, empfiehlt es sich, bei Beschlussbeantragung eine gesonderte Ausfertigung des Beschlusses zur Vorlage bei dem betroffenen Dritten zu erfragen. Diese Beschlussausfertigung sollte nur

- das Gericht,
- Datum,
- Aktenzeichen,
- die Rechtsgrundlage und
- den Beschuldigten nennen sowie
- gegebenenfalls die Verpflichtung des Dritten zur Verschwiegenheit aussprechen.

Allein wegen des Grundsatzes der Subsidiarität waren bei allen betrachteten Verfahren Wohnraumüberwachungsmaßnahmen erst dann und nur deshalb beantragt worden, weil andere operative Maßnahmen ohne Ermittlungserfolg geblieben waren.

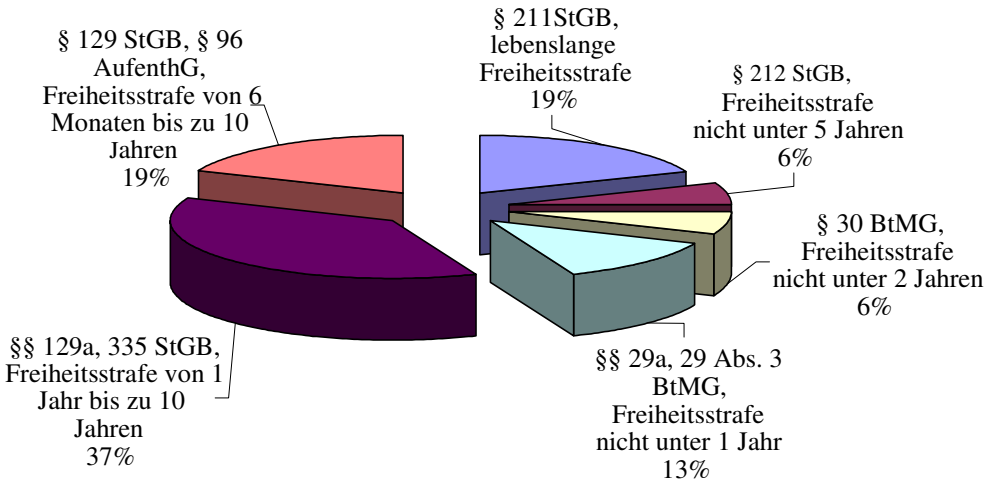
1.4. Anlasstaten

Bezüglich der Katalogtaten, die Anlass für Beschlüsse nach § 100c StPO waren, ergab die Erhebung eine sehr heterogene Verteilung. Eine signifikante Aussage kann daher nicht getroffen werden. In der folgenden Grafik werden die Delikte, nach ihrer Strafandrohung unterschieden, dargestellt.

Anlasstaten für Beschlüsse nach § 100c StPO

	Häufigkeit	Prozent
lebenslange Freiheitsstrafe, § 211 StGB	3	19 %
Freiheitsstrafe von 1 Jahr bis zu 10 Jahren §§ 129a, 335 StGB	6	37 %
Freiheitsstrafe von 6 Monaten bis zu 10 Jahren § 129 StGB, § 96 AufenthG	3	19 %
Freiheitsstrafe nicht unter 5 Jahren, § 212 StGB	1	6 %
Freiheitsstrafe nicht unter 2 Jahren § 30 BtMG	1	6 %
Freiheitsstrafe nicht unter 1 Jahr §§ 29a, 29 III BtMG	2	13 %
Gesamt	**16**	**100 %**

In zwei der untersuchten Verfahren wurde nur deswegen eine Wohnraumüberwachung durchgeführt, weil bei Bestechungsdelikten eine Telekommunikationsüberwachungsmaßnahme nicht zulässig war. Daher ist die kürzlich erfolgte Aufnahme von Bestechungsdelikten in den Katalog[21] von § 100a StPO zu begrüßen.



1.5. Betroffene Personen; Relevanz für die Benachrichtigungspflicht

Bei den durch die Maßnahmen Betroffenen ist zwischen den Beschuldigten des konkreten Verfahrens und Dritten, also allen Personen außer dem Beschuldigten, zu differenzieren.

Die Auswertung des Projekts ergab, dass **Dritte** durch Maßnahmen zur akustischen Wohnraumüberwachung oftmals nur in **geringem Maß** betroffen waren. Hinsichtlich Dritter kann zwischen unerheblich und erheblich Betroffenen unterschieden werden.

Erheblich betroffene Dritte sind beispielsweise der Inhaber einer überwachten Wohnung selbst, der keine Zielperson ist, sowie Kontakt- oder Begleitpersonen. Erheblich betroffen waren in den untersuchten Verfahren in drei Fällen jeweils eine Person, in einem Verfahren zwei Personen und in einem weiteren Verfahren fünf Personen.

[21] Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21.12.2007 (BGBl. 2007 I S. 3198).

Lediglich **unerheblich betroffen** sind Personen, die nur zufälligen Kontakt zu erheblich Betroffenen hatten, z.B. als Briefträger oder Pizzabote. Das betraf in zwei Verfahren jeweils zwei und in je einem Verfahren eine, fünf bzw. acht Personen.

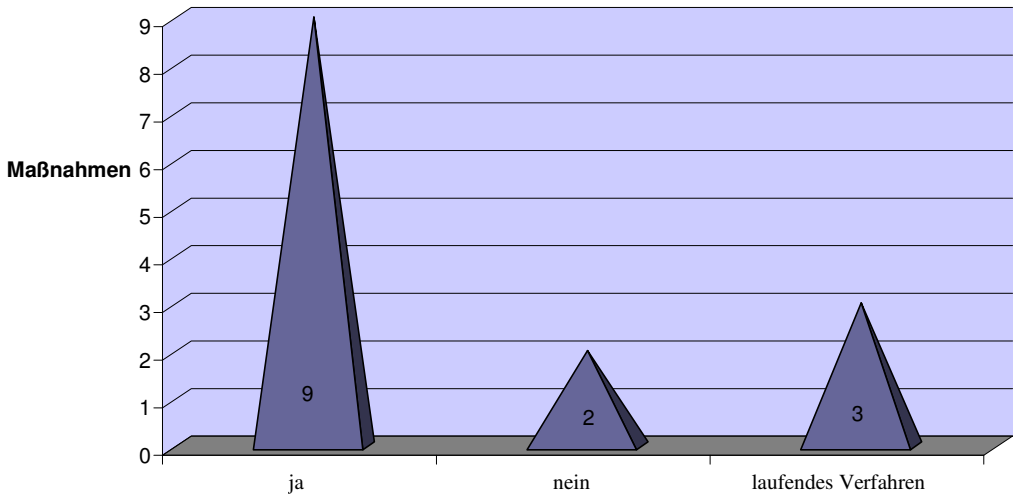
In zwei Verfahren waren jeweils die Ehepartner sowie die Geschwister der Beschuldigten betroffene Dritte. Die Betroffenen waren jeweils einer Beteiligung verdächtig, so dass die Wohnraumüberwachung nach § 100c Abs. 6 Satz 3 StPO zulässig war.

Die **Benachrichtigung** ist zwar grundsätzlich Aufgabe der Justiz, gleichwohl hat oftmals die Polizei die notwendigen vorbereitenden Leistungen in Form einer Auflistung der betroffenen Personen zu erbringen. Außerdem sind für die Prüfung einer etwaigen Zurückstellung der Benachrichtigung oftmals polizeiliche Erkenntnisse und Einschätzungen beizubringen.

Benachrichtigung Betroffener

	Häufigkeit	Prozent	Gültige Prozente
ja	9	56,3 %	64,3 %
laufendes Verfahren	3	18,7 %	21,4 %
nein	2	12,5 %	14,3 %
Gesamt	14	87,5 %	**100 %**
keine Angaben (Maßnahme wurde nicht durchgeführt, da kein Beschluss erlassen worden war)	2	12,5 %	
Gesamt	**16**	**100 %**	

In der überwiegenden Zahl der untersuchten Verfahren, in neun von 14 Fällen, wurden alle Betroffenen über die Durchführung der Maßnahme benachrichtigt. Drei Ermittlungsverfahren waren zum Zeitpunkt der Datenerhebung noch nicht abgeschlossen, so dass aus diesem Grund eine Benachrichtigung noch nicht erfolgt war. In lediglich zwei Verfahren wurden Betroffene nach Verfahrensabschluss nicht benachrichtigt, um den Ermittlungserfolg bzw. einen eingesetzten Verdeckten Ermittler nicht zu gefährden.



Die **Neuregelung der Benachrichtigungspflichten**[22] im Fall verdeckter Maßnahmen in § 101 StPO hat den Kreis der zu benachrichtigenden Personen aus § 100d Abs. 8 StPO a.F. nicht verändert.

Neu gefasst wurde allerdings das Unterbleiben der Benachrichtigung, wenn ihr überwiegend schutzwürdige Belange einer betroffenen Person entgegenstehen. Nachforschungen zur Feststellung der Identität der Personen sind bei allen eigentlich zu Benachrichtigenden – und nicht mehr nur unerheblich Betroffenen – nur vorzunehmen, wenn dies unter Berücksichtigung der Eingriffsintensität der Maßnahme gegenüber dieser Person, des Aufwandes für die Feststellung ihrer Identität sowie der daraus für diese oder andere Personen folgenden Beeinträchtigungen geboten ist.

Eine Benachrichtigung hat, wie nach alter Rechtslage auch, binnen sechs Monaten nach Beendigung der Maßnahme zu erfolgen. Eine längere Zurückstellung bedarf gemäß § 101 Abs. 6 StPO der gerichtlichen Zustimmung.

1.6. Dauer der Maßnahmen

Gerichtlich **angeordnet** wurde die Wohnraumüberwachung in der überwiegenden Zahl der Fälle – in neun von 15 Verfahren – für eine **Dauer von bis zu 30 Tagen**.

[22] Durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21.12.2007, BGBl. 2007 I S. 3198.

Maximale Dauer (einschließlich Verlängerung) der Wohnraumüberwachung laut Anordnung

(in Tagen)	Häufigkeit	Prozent
3	1	6,7 %
14	1	6,7 %
19	1	6,7 %
28	5	33,2 %
30	1	6,7 %
56	1	6,7 %
60	1	6,7 %
84	2	13,2 %
112	1	6,7 %
280	1	6,7 %
Gesamt	**15**	**100 %**

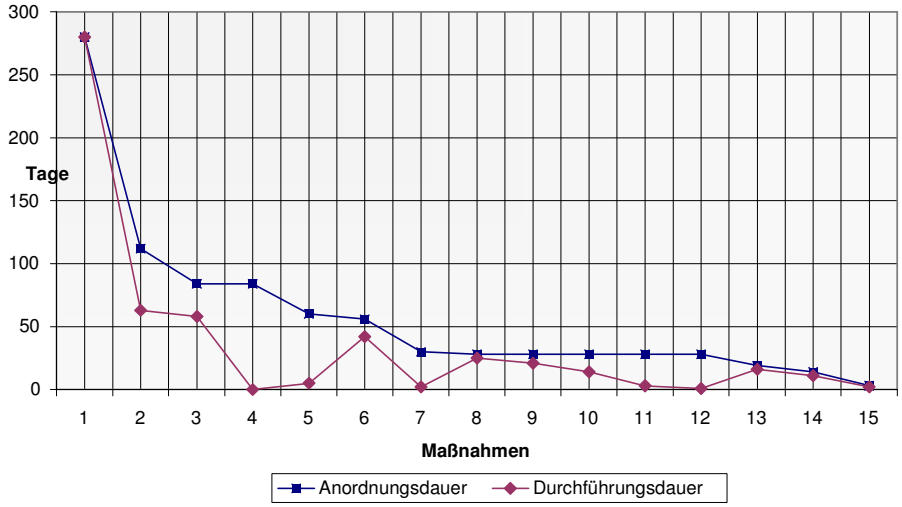
Tatsächlich erfolgte die Überwachung des jeweiligen Wohnraums weitaus kürzer, als dies der richterlichen Anordnung nach zulässig gewesen wäre. In zehn Fällen dauerten die Überwachungsmaßnahmen weniger als vier Wochen an, nur in vier Fällen wurde eine Wohnraumüberwachung länger als vier Wochen durchgeführt.

Tatsächliche Dauer der Wohnraumüberwachung

(in Tagen)	Häufigkeit	Prozent
0,08	1	7,15 %
2	2	14,2 %
3	1	7,15 %
5	1	7,15 %
11	1	7,15 %
14	1	7,15 %
16	1	7,15 %
21	1	7,15 %
25	1	7,15 %
42	1	7,15 %
58	1	7,15 %
63	1	7,15 %
280	1	7,15 %
Gesamt	**14**	**100 %**

Diese Ergebnisse führen zu der Erkenntnis, dass § 100c StPO in der Praxis restriktiv gehandhabt wird. Zum einen werden Beschlüsse nur noch für kurze Zeiträume, z.B. nur drei Tage, beantragt bzw. erlassen. Zum anderen wird der genehmigte Zeitraum in aller Regel nicht voll ausgeschöpft, sondern die Überwachung früher beendet. Gesetzlich sind die Strafverfolgungsbehörden bei der Wohnraumüberwachung (ebenso wie z.B. bei anderen verdeckten Maßnahmen, etwa der TKÜ) ohnehin zwingend gehalten, bei Wegfall der Erforderlichkeit die Maßnahme sofort zu beenden.

Vergleich der Anordnungsdauer zu der tatsächlichen Dauer der Maßnahme



Diese restriktive Praxis der akustischen Wohnraumüberwachung ist einerseits bedingt durch das Gebot der Verhältnismäßigkeit, wonach eine Wohnraumüberwachung nicht länger als unbedingt erforderlich durchgeführt werden darf. Andererseits ist diese Zurückhaltung jedoch auch dem hohen Personal- und Finanzaufwand geschuldet, mit dem solche Maßnahmen verbunden sind.

1.7. Kernbereich privater Lebensgestaltung

Das zunächst vom BVerfG aufgestellte und später bei der Novellierung in die StPO aufgenommene Gebot des Schutzes des Kernbereichs privater Lebensgestaltung basiert auf dem Grundsatz, dass jedem Bürger eine Rückzugssphäre zugestanden werden muss, sozusagen ein letzter unantastbarer Bereich menschlicher Freiheit. Was genau unter dem Kernbereich privater Lebensgestaltung zu verstehen ist, wurde gesetzlich nicht eindeutig beschrieben. Vielmehr hat der Gesetzgeber nur bestimmte Rahmenbestimmungen getroffen, die regeln, wann typischerweise eine Maßnahme nicht in den Kernbereich privater Lebensgestaltung eingreift.[23]

Nach der Rechtsprechung des BVerfG[24] umfasst der Kernbereich privater Lebensgestaltung jeden inneren Vorgang wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art. Daneben sind auch Gefühlsäußerungen,

[23] Vgl. dazu 1.7.1..
[24] Vgl. BVerfGE 109, 279 (313 f.).

Äußerungen des unbewussten Erlebens sowie Ausdrucksformen der Sexualität erfasst. Indiz für eine Nichtbetroffenheit des Kernbereichs privater Lebensgestaltung und dafür, dass ein Verhalten keinen höchstpersönlichen Charakter besitzt, ist der Umstand, dass der Vorgang **die Sphäre anderer oder die Belange der Gemeinschaft berührt**.

In den analysierten Verfahren wurden als Situationen mit eindeutigem Kernbereichsbezug in vier Verfahren Ausdrucksformen der Sexualität genannt.

Dabei wurde die **Kernbereichsrelevanz** durch die jeweilige sachbearbeitende Dienststelle zum Beispiel in folgenden Situationen als für die Entscheidung problematisch erachtet:

- Selbstgespräche
- Gebete
- Gespräche über die Religionszugehörigkeit der jeweiligen Personen
- Gespräche über die Erziehung eines Kindes,
- Gespräche unter Eheleuten abhängig vom Gesprächsinhalt.

Zu den vorgenannten exemplarisch aufgeführten Fallkonstellationen sind folgende Erwägungen vorzunehmen:
Eine gerichtliche Klärung bezüglich der Zugehörigkeit eines **Selbstgesprächs** zum Kernbereich privater Lebensgestaltung hat mittlerweile der BGH in der so genannten „Krankenzimmerentscheidung“[25] vorgenommen. Er kommt zu dem Ergebnis, dass ein Gespräch mit sich selbst gekennzeichnet sei durch unwillkürlich auftretende Bewusstseinsinhalte und persönliche Erwartungen, Befürchtungen, Bewertungen, Selbstanweisungen sowie seelisch-körperliche Gefühle und Befindlichkeiten zum Inhalt habe. Bemerkenswert war in dem zu entscheidenden Fall, dass das Selbstgespräch tatrelevant war, da es in ihm um eine begangene Straftat ging, und solche Gespräche gemäß § 100c Abs. 4 Satz 3 StPO in der Regel nicht dem Kernbereichsschutz unterfallen. Insofern argumentierte der BGH aber, dass ein Selbstgespräch kein echtes „Gespräch“ darstelle, da es nicht dazu bestimmt sei, von anderen zur Kenntnis genommen zu werden. Daher liege im betreffenden Fall auch keine Gemengelage eines Gesprächs mit höchstpersönlichem und straftatbezogenem Inhalt vor, so dass eine Abwägung nicht erforderlich sei.

[25] BGH NJW 2005, 3295.

In Folge dieses Urteils haben mehrere Beschlüsse Selbstgespräche explizit von der Überwachungsanordnung ausgenommen. Ob sich diese Rechtsprechung weiter verfestigt, bleibt abzuwarten.

Bei Selbstgesprächen – es ist nur eine Person im zu überwachenden Objekt anwesend – ist nach der bisherigen Rechtsprechung eine Aufzeichnung unzulässig, unabhängig vom Inhalt des Selbstgesprächs.

In einem Beschluss eines Oberlandesgerichts vom August 2007 wurde von der Verwertung aufgezeichneter Selbstgespräche daher abgesehen:

> *„Bedenken an einer Verwertbarkeit einzelner Gespräche bestehen hinsichtlich derjenigen Zeiträume, in denen sich der Angeklagte allein in der zu überwachenden Wohnung befand. In dieser Zeit las der Angeklagte offenbar „sich selbst" aus Briefen bzw. Briefentwürfen vor, die er an dritte Personen verfasst hatte. Der Senat sieht von der Verwertung dieser „Gespräche" ab.*
>
> *Vor diesem Hintergrund bestehen auch Bedenken gegen die Verwertbarkeit von Zitaten aus schriftlichen Aufzeichnungen, deren Schicksal (Absendung, Aufbewahrung oder Vernichtung) ungeklärt geblieben ist. Trotz des ermittlungsbezogenen Inhalts werden sie vorsorglich als Beweismittel ausgeschlossen."*

Gespräche **über religiöse Themen** sowie Gebete, die keine Selbstgespräche waren, wurden durch ein Gericht im Rahmen eines Senatsbeschlusses im September 2007 als außerhalb des Kernbereichs privater Lebensgestaltung liegend betrachtet, soweit sie allgemeine Fragen der Mythologie sowie Glaubensausübung betrafen. Hierzu Auszüge aus einem Beschluss:

> *„Die Aufzeichnung von „Gebetspassagen" stellt keine Verletzung des Kernbereichs privater Lebensgestaltung dar. Das Gebet als spirituelle Auseinandersetzung mit einer göttlichen Macht trägt nämlich nicht stets höchstpersönlichen Charakter. Es weist vielmehr Sozialbezug auf, wenn der Betende bei der Gebetsverrichtung auf persönliche Isolation gerade verzichtet, indem er beim Gebet die Gemeinsamkeit mit anderen Gläubigen sucht oder zumindest ein Mithören durch weitere Personen bewusst in Kauf nimmt."*

Gespräche über religiöse Themen sowie Gebete, die keine Selbstgespräche sind, sind als nicht kernbereichsrelevant zu erachten, wenn sie allgemeiner Natur sind. Beispielsweise das Beten des „Vater unser“ oder einer Koransure dürften nicht dem Kernbereich unterfallen, da der Inhalt nicht höchstpersönlicher Natur ist. Individuelle Gebete gehören dagegen im Zweifel zum Kernbereich privater Lebensgestaltung, sofern in ihnen nicht tatbezogene Inhalte thematisiert werden bzw. zu erwarten sind.

Eine abstrakte Einordnung von Situationen, ob sie zum Kernbereich privater Lebensgestaltung gehören oder nicht, stellt einen untauglichen und allenfalls akademischen Versuch dar. Ein Gespräch über z.B. besondere sexuelle Neigungen kann bei einem Tatverdächtigen kernbereichs-, bei einem Sexualstraftäter jedoch tatrelevant sein.[26] Daher ist eine **einzelfallbezogene Bewertung** der jeweiligen Situation erforderlich.

Grundsätzlich besteht in der gerichtlichen Anordnung zwar die Möglichkeit, hinsichtlich der Kernbereichsrelevanz von Situationen zwischen **einzelnen Räumen** innerhalb eines überwachten Objektes zu differenzieren. So wurden z.B. durch ein Landgericht Toilettenräume ausgenommen. Technisch ist eine solche Differenzierung jedoch in der Regel nicht umzusetzen, da die installierten Sender die Herkunft der Audio-Signale nicht erkennen können.

Die untersuchte polizeiliche Praxis hat überdies gezeigt, dass ein Erkennen einer Kernbereichsverletzung durch die Verwendung kryptierter Sprache und bei Gesprächen in fremder Sprache besonders erschwert wird.[27] Auf die Ausführungen unter Punkt 1.8. zu diesem Themenfeld wird verwiesen.

1.7.1. Prognose zur Betroffenheit des Kernbereichs privater Lebensgestaltung

Bevor eine Maßnahme nach § 100c StPO beantragt werden kann, ist eine Prognoseerstellung hinsichtlich der Kernbereichsrelevanz erforderlich. Für die **Prognose**, ob es zu einer Kernbereichsbetroffenheit kommen kann, gibt § 100c Abs. 4 StPO Indikatoren vor. Im Rahmen der so genannten negativen Kernbereichsprognose kommt der Art der zu überwachenden Räumlichkeiten, dem Verhältnis der Personen zueinander sowie Gesprächen über Straftaten Indizwirkung zu. Als grobe Richtlinie kann angenommen

[26] Vgl. BVerfG (2 BvR 518/07) zur Beschlagnahme von Tagebüchern mit Schilderungen sexueller Handlungen mit Kindern. Das hohe öffentliche Interesse an einer wirksamen Strafverfolgung rechtfertige die Beschlagnahme, wenn sie nicht von vornherein ausgeschlossen sei.

[27] Dies erkennt das BVerfG in dem Urteil zur Online-Durchsuchung, NJW 2008, 822 (834) an.

werden: Je vertrauter eine Situation bzw. Umgebung ist, desto eher ist der Kernbereich privater Lebensgestaltung betroffen.

- Zunächst ist die **Art der zu überwachenden Räume** zu beachten, wobei zwischen den bereits aufgezeigten Arten von Räumlichkeiten unterschieden wird.

  - Sollen **Privatwohnungen** überwacht werden, spricht eine grundsätzliche Vermutung für die Vertraulichkeit der darin stattfindenden Interaktionen (§ 100c Abs. 4 Satz 1 StPO), da Privatwohnungen typischerweise der Rückzugsbereich des Einzelnen sind. Diese Vermutung kann aber durch konkrete Erkenntnisse widerlegt werden.[28] Insoweit besteht ein Regel-Ausnahme-Verhältnis.

    Indizien für eine Bestimmung von Räumen zu Wohnzwecken (Wohnung im engeren Sinne) sind das Vorhandensein eines Privatbereichs, der durch Abgeschlossenheit und Öffentlichkeitsausschluss gekennzeichnet ist, in dem sich das Privatleben ungestört entfalten kann.

  - Bei der Überwachung von **Arbeits-, Betriebs- und Geschäftsräumen** ist dagegen zu vermuten, dass der Kernbereich nicht betroffen ist (§ 100c Abs. 4 Satz 2 StPO), da ihnen die Vertrautheit und Geborgenheit der Privatwohnung fehlt.

    Indizien für einen Betriebs- und Geschäftsraum (Wohnung im weiteren Sinne) sind ungehinderter Zugang zu den Räumlichkeiten, also Publikumsverkehr, offene Türen, Zutrittsberechtigung für jedermann, allgemeine Öffnungszeiten, z.B. ein allgemein zugängliches Vereinsbüro[29], die tatsächliche Nutzung der Räume als Büroräume sowie das Fehlen jeglicher Anhaltspunkte für eine räumliche Privatsphäre der Nutzungsberechtigten.

  - Bei Räumen, die **gleichzeitig Arbeits- und Wohnzwecken** dienen, greift keine Vermutung ein, so dass es hier ausschließlich auf das Vorliegen anderer Indikatoren ankommt.

[28] Eine als konspirativer Treffpunkt oder im konkreten Fall zu betrieblichen Zwecken genutzte oder eine der Ausübung der Prostitution dienende Privatwohnung wird in der Regel nicht dieser Vermutung unterfallen, vgl. BT-Drs. 15/4533, S. 14.

[29] Vgl. BGHSt 42, 372.

Eine **Unterscheidung innerhalb eines Objektes** in Räume mit privater Nutzung und ohne eine solche Nutzung ist in der Regel **nicht möglich** und wäre im Übrigen – wie bereits dargestellt – auch technisch nur schwer umzusetzen

Daher ist eine einheitliche Bewertung für die gesamte Örtlichkeit, die überwacht werden soll, angezeigt. Dies bedeutet auch, dass bei einem Objekt, in dem sowohl ABG-Räume als auch private Wohnräume vorhanden sind, beispielsweise bei einem Verkaufsladen mit Schlafgelegenheit im Hinterzimmer, eine einheitliche Entscheidung bezogen auf das gesamte Objekt getroffen werden muss.

Eine etwaige richterliche Vorgabe, bestimmte Teile einer Räumlichkeit von der Überwachung auszunehmen, ist nur schwer umzusetzen; einer solchen Differenzierung sollte schon in der Anregung/Beantragung im Hinblick auf die technischen Möglichkeiten entgegen gewirkt werden.

- Des Weiteren ist das **Verhältnis der beteiligten Personen zueinander** zu beachten. Schutzwürdig ist die Kommunikation zwischen so genannten Personen des Vertrauens. Zwischen welchen Personen ein Vertrauensverhältnis besteht, ist vom Gesetzgeber nicht vorgegeben, hat sich jedoch ausweislich der Rechtsprechung des BVerfG[30] sowohl nach formalen Gesichtspunkten als auch nach tatsächlichem Vertrauen zu bestimmen.
    - Als **formal schutzwürdige Personen** gelten i.d.R. Eheleute und Familienangehörige wie Geschwister sowie Verwandte in gerader Linie, insbesondere, wenn sie im selben Haushalt wie die Zielperson leben.
    - Personen **besonderen Vertrauens** sind typischerweise z.B. enge persönliche Freunde sowie Berater wie beispielsweise Strafverteidiger, Geistliche und im Einzelfall auch Ärzte.[31]

  Ein Widerlegen der Vermutung, dass es hierbei zu kernbereichsrelevanten Situationen kommen kann, ist schwierig und gelingt in der Regel anhand der für die Bewertung erforderlichen Indizien nur dann, wenn die anwesenden Personen entweder selbst tatverdächtig oder als Kontakt- oder Begleitpersonen anzusehen sind.

[30] BVerfGE 109, 279 (322 f.).
[31] BVerfGE 109, 279 (323).

Kontakt- oder Begleitperson ist eine Person jedenfalls dann, wenn sie mit einem Tatverdächtigen in einer Weise in Verbindung steht, die erwarten lässt, dass durch diese Person Hinweise über die mutmaßliche Straftat gewonnen werden können, und zwar deshalb, weil Tatsachen die Annahme rechtfertigen, dass die Person insbesondere von der Planung oder der Vorbereitung der Straftat, von der Verwertung der Tatvorteile oder von einer einzelnen Vorbereitungshandlung Kenntnis hat oder daran sogar wissentlich oder unwissentlich mitwirkt.[32]

In einem konkreten Verfahren bestanden bei der Überwachung eines Zimmers in einer Wohngemeinschaft, das gleichzeitig Schlaf- und Wohnzimmer war, zunächst Bedenken hinsichtlich der Zulässigkeit der Maßnahme, welche zwischen Polizei, Staatsanwaltschaft und dem zuständigen Ermittlungsrichter diskutiert wurden. Aufgrund des Nachweises, dass der Beschuldigte zum Überwachungszeitpunkt Single war und auch sonst keine Anhaltspunkte für eine Kernbereichsrelevanz bestanden, wurde jedoch der Beschluss nach § 100c StPO genehmigt.

Gleichwohl bedeutet die bloße Anwesenheit von Personen des Vertrauens keinen kategorischen Ausschluss der Wohnraumüberwachung. Dass auch bei Eheleuten eine Wohnraumüberwachung zulässig sein kann, zeigt der Auszug aus zwei Beschlüssen nach § 100c StPO. Hier waren allerdings beide Eheleute Beschuldigte, d.h. aufgrund von straftatenrelevanten Gesprächsinhalten ist im Einzelfall der unantastbare Kernbereich selbst bei Eheleuten nicht betroffen.

Auszüge:

> *„Die bereits beantragte, genehmigte und seit ... geschaltete Telefonüberwachung des Festnetzanschlusses sowie des Handys des … ergab nach Aktenlage bislang keine wesentlichen Erkenntnisse, da die Beschuldigten kaum, und wenn, dann nicht über dieses Thema, miteinander telefonisch kommunizieren und insoweit auch nicht dritte Personen in die Tat einweihen. Eine Aufklärung durch Einschaltung einer Vertrauensperson oder gar eines verdeckten Ermittlers erscheint von vornherein völlig aussichtslos, da die Tat den engsten familiären Kreis betrifft, in den außen stehende Personen nach der allgemeinen Lebenserfahrung nicht eingeweiht werden.“*

[32] Angelehnt an § 2 Nr. 12 Niedersächsisches SOG.

oder:

> *„Bei dem von der Maßnahme betroffenen Objekt handelt es sich um die Wohnung der Eheleute, die ausschließlich von den beiden Beschuldigten bewohnt wird. Diese hat an sich die Funktion als Rückzugsbereich der privaten Lebensgestaltung und wäre damit einer akustischen Wohnraumüberwachung im Regelfall nicht zugänglich, da von den konkreten Verhältnissen her – die Beschuldigten sind Eheleute, das zu überwachende Objekt die von beiden gemeinsam bewohnte Ehewohnung – grundsätzlich zu erwarten ist, dass durch die Maßnahme auch Äußerungen erfasst werden können, die dem unantastbaren Kernbereich privater Lebensführung zuzuordnen sind und damit dem Schutzbereich der Art. 13 Abs. 1, 1 Abs. 1, 2 Abs. 1, 6 Abs. 1 GG unterfallen. § 100c Abs. 3 StPO stellt jedoch ausdrücklich klar, dass Gespräche über begangene Straftaten und Äußerungen hierüber nicht dem Kernbereich privater Lebensgestaltung zuzurechnen sind. Dies gilt auch dann, wenn die Maßnahme Personen betrifft, die zueinander zusätzlich noch in einem besonderen höchstpersönlichen Vertrauensverhältnis stehen.“*

- Schließlich unterfallen **Gespräche über begangene Straftaten**, unabhängig davon, zwischen welchen Personen und in welcher Räumlichkeit sie geführt werden, nicht dem Kernbereich privater Lebensgestaltung (§ 100c Abs. 4 Satz 3 StPO)[33], dabei hat der BGH im Fall von Selbstgesprächen (s.o.) insoweit eine Grenze gesetzt.

  Gerichtliche Beschlüsse wurden z.B. mit folgender Begründung erlassen:

  > *„Art und Weise der Durchführung der Maßnahme kann so ausgestaltet werden, dass die akustische Überwachung des Wohnraums des Beschuldigten nicht in dessen absolut geschützten Kernbereich privater Lebensgestaltung eingreift. Diese Gefahr besteht nach den bisher bekannten Umständen nicht, weil der Beschuldigte seine Wohnung alleine bewohnt. Im Übrigen hat er keine feste Partnerin oder Lebensgefährtin, keine Kinder oder enge Verwandte, die in der Wohnung leben oder ihn dort (regelmäßig) aufsuchen. Gerade und insbesondere bei seinen Treffen mit den anderen Beschuldigten ist nicht zu erwarten, dass die absolut geschützte Persönlichkeitssphäre berührt wird, weil die zu führenden strafrechtlich relevanten Gespräche sich lediglich auf Straftaten beziehen werden, also keinerlei Grundrechtsschutz unterliegen.*
  > *Die Überwachung wird mit der Maßgabe genehmigt, dass durch geeignete Maßnahmen sichergestellt wird, den gesetzlichen Vorgaben des § 100c Abs. 5 und Abs. 6 StPO zu genügen.“*

[33] BVerfGE 109, 279 (319).

oder:

> *„Dass durch die Durchführung der Maßnahme in unzulässiger Weise Äußerungen erfasst werden, die dem Kernbereich der privaten Lebensgestaltung unterliegen, ist nicht anzunehmen. Ob die überwachten Äußerungen dem Bereich des Höchstpersönlichen zuzurechnen sind oder nicht, kann regelmäßig erst bei oder nach Durchführung der Überwachung beurteilt werden. Der Schutz des Kernbereichs privater Lebensgestaltung fordert deshalb, dass vor Maßnahmen akustischer Wohnraumüberwachung tatsächliche Anhaltspunkte gegeben sind, aus denen zumindest in typisierender Weise geschlossen werden kann, dass die zu überwachenden Gespräche nicht dem höchstpersönlichen Bereich zugeordnet werden können. Solche konkreten Anhaltspunkte liegen hier vor.“ (Anmerkung: Die Überwachungsmaßnahme war direkt im Anschluss an eine Vernehmung beider Beschuldigter geplant, so dass zu erwarten war, dass diese sich über die Vernehmung bzw. die Tat unterhalten werden und damit der kernbereichsausschließende Straftatenbezug gegeben war).*

Zum Schutz des Kernbereichs privater Lebensgestaltung haben Gerichte in Einzelfallentscheidungen vorgegeben, dass eine Überwachung der Wohnung des Beschuldigten oder eines Dritten bei Anwesenheit des Beschuldigten nur zulässig ist, **wenn bestimmte Personen im Objekt anwesend sind**, wobei zum Zweck der permanenten Kernbereichsüberprüfung durch flankierende Maßnahmen der Charakter des Verhältnisses der anwesenden Personen zueinander bewertet werden muss, oder aber wenn bei bestimmten vorher durch die Anordnung festgelegten Personen keine Gefahr der Kernbereichsverletzung zu erwarten ist.

Eine Identifizierung der in der Wohnung ein- und ausgehenden Personen lässt sich aber nur durch Ermittlungen im Außenbereich eines Objektes realisieren, z.B. mittels stationärer Videotechnik bzw. eines Einsatzes von Observationskräften vor den Objekteingängen. Hier kommt es zu den gleichen Problemen, wie sie im Zusammenhang mit den flankierenden Vorbereitungsmaßnahmen bereits erwähnt wurden. So ist der Erfolg einer solchen Identifizierung beispielsweise abhängig von den örtlichen Gegebenheiten und kann dadurch vereitelt werden, dass der zu beobachtende Zugang durch vorbeifahrende Fahrzeuge oder Ähnliches verdeckt wird.

Im gerichtlichen Beschluss lautete die Anordnung:

> *„Eine Ausforschung des unantastbaren Kernbereichs privater Lebensgestaltung ist durch die Wohnraumüberwachung im vorliegenden Fall nicht mit Wahrscheinlichkeit zu erwarten. Sie soll zwar in einer Privatwohnung durchgeführt werden, bei der es sich jedoch mit hoher Wahrscheinlichkeit um einen Ort zur Vorbereitung einer Straftat handelt und in dem keine regelmäßigen Besuche von persönlich nahe stehenden Personen, insbesondere Verwandten oder Freunden, die nicht derselben Tätergruppe zuzurechnen sind, zu erwarten sind. Dabei kann sichergestellt werden, dass aufgrund der zeitgleichen Observationsmaßnahmen eine engmaschige Kontrolle der diese Wohnung betretenden Personen gewährleistet wird."*

Gerade dieses Beispiel macht deutlich, dass auf der Anordnungsebene keine zu strengen Maßstäbe angelegt werden sollten, wenn der Kernbereichsschutz bei der Durchführung der Maßnahme umfassend gewährleistet werden kann.

Die Videoüberwachung war jedoch in einem konkreten Ermittlungsverfahren nicht zu realisieren: In diesem Fall war nämlich die Zahl der möglichen Objektzugänge so hoch, dass eine lückenlose Beobachtung nicht möglich war und daher auch im Beschluss explizit vom Erfordernis der Videoüberwachung abgesehen wurde. Indizien für die Anbahnung kernbereichsrelevanter Situationen konnten durch Begleitmaßnahmen somit nicht erlangt werden. Die Kernbereichsrelevanz war daher ausschließlich durch Kenntniserlangung des gesprochenen Wortes in der Wohnung zu bewerten.

Der hohe Aufwand für die Überwachung von außen bedingt nicht nur einen hohen Personaleinsatz, sondern erhöht auch das Entdeckungsrisiko der Maßnahme. Dies gilt wegen des Erfordernisses einer Prognoseerstellung sogar schon vor dem Beginn der eigentlichen Maßnahme, z.B. bei der Voraufklärung des Objektes.
In letzter Konsequenz ist es denkbar, dass eine Wohnraumüberwachung nicht durchgeführt werden kann, weil eine Videoüberwachung aufgrund der Besonderheiten des Wohnumfeldes (z.B. sensibilisierte Nachbarschaft) nicht unentdeckt installiert werden kann.

Die Videoüberwachung im Außenbereich kann folglich eine herausragende Rolle zur Absicherung des Kernbereichs spielen. Insbesondere wenn sie nicht durchgeführt werden kann, müssen andere flankierende Maßnahmen zur Prognosestellung und zur Überprüfung der Kernbereichsrelevanz des aufgezeichneten gesprochenen Wortes in der Wohnung weiter genutzt werden.

Damit offenbart sich eine Paradoxie: Zum effektiven Schutz des Kernbereichs müssen weitere Maßnahmen durchgeführt werden, wodurch sich der Eingriff in die Privatsphäre des Betroffenen vertieft. Eine strenge Auslegung des Kernbereichsschutzes kann also zu einer umfassenderen Überwachung führen.

1.7.2. Schutz des Kernbereichs privater Lebensgestaltung

1.7.2.1. Erfordernis des Live-Mithörens

In den untersuchten Fällen traf man jeweils die Prognose, dass eine überwiegende Wahrscheinlichkeit dafür besteht, dass der Kernbereich nicht betroffen sein wird. Dies lag z.B. an der Art des überwachten Objektes (eine Wohnung, die nur zur Verabredung von Straftaten genutzt wurde) oder an dem Überwachungszeitpunkt (direkt nach einer Vernehmung beider Beschuldigter, weshalb damit gerechnet werden konnte, dass es Gespräche über die Tat geben wird).
Dennoch wurde zur Gewährleistung des Schutzes des Kernbereichs privater Lebensgestaltung meist eine automatisierte Datenspeicherung nicht gefordert. Vor allem bei Maßnahmen in Privatwohnungen –in acht von elf Verfahren in Privatwohnungen – wurde ein **Live-Mithören** angeordnet. Dies sollte garantieren, dass die Aufnahme sofort gestoppt werden konnte, wenn entgegen der zuvor gestellten Prognose eine Kernbereichsverletzung eintreten sollte.

Anordnung eines Live-Mithörens abhängig von der Art des Raumes

			Auf welche Art von Räumen bezog sich die Überwachung?			Gesamt
			Privat-wohnung	sonstiger geschützter Raum	ABG-Raum	
Live-Mithören angeordnet?	ja	Anzahl	8	0	2	**10**
	nein	Anzahl	3	1	1*	**5**
Gesamt		Anzahl	11	1	3	**15**

* Die Maßnahme wurde nicht realisiert.

Aber auch in den ebenfalls von § 100c StPO erfassten Arbeits-, Betriebs- und Geschäftsräumen sowie sonstigen geschützten Räumen wurde in zwei von drei untersuchten Fällen ein Live-Mithören angeordnet, obwohl dort die Wahrscheinlichkeit kernbereichsrelevanter Situationen geringer einzustufen ist als bei Maßnahmen in Privatwohnungen.

Ein „Live-Schichtbetrieb“ bedeutet die ständige Anwesenheit eines Sachbearbeiters der Dienststelle sowie bei fremdsprachigen Gesprächen ggf. die eines Dolmetschers.
In richterlichen Beschlüssen wurde dies so formuliert:

> *„Gemäß §§ 100c, 100d StPO wird das Abhören und Aufzeichnen des nichtöffentlich gesprochenen Wortes in der Wohnung des Beschuldigten … im Wege der Echtzeitüberwachung über 24 Stunden täglich durch in den Räumen der Wohnung angebrachte Abhör- und Sendevorrichtungen für die Dauer von … angeordnet.“*

oder:

> *„Die Maßnahme ist in Echtzeit, d.h. unter gleichzeitigem Mithören durch das Überwachungspersonal durchzuführen. Das Abhören und Aufzeichnen ist sofort zu unterbrechen, sobald im Rahmen der Maßnahme in der Wohnung des Beschuldigten zum Beispiel die Anwesenheit von Prostituierten festgestellt wird und durch die Fortführung der Maßnahme der Kernbereich der privaten Lebensgestaltung des Beschuldigten betroffen sein kann. Eine Fortführung der Maßnahme ist in diesem Fall erst dann wieder zulässig, wenn aufgrund anderer Maßnahmen – etwa einer Observation der betroffenen Wohnung – sichere Erkenntnisse darüber vorliegen, dass eine Verletzung des Kernbereichs ausgeschlossen ist.“*

Um eine einheitliche und den verfassungsrechtlichen Erfordernissen entsprechende Vorgehensweise zur Wahrung des Kernbereichsschutzes zu gewährleisten, ist aus Sicht des Projektteams das Erstellen von "Leitfäden" für die mit der Durchführung der Maßnahme, insbesondere der Echtzeitüberwachung, betrauten Sachbearbeiter hilfreich. .
Obgleich jede Fallkonstellation einzelfallabhängig bewertet werden muss, sollten h.E. diesen Kräften aus Gründen der Rechtssicherheit Indizien und Kriterien für die Bewertung der Kernbereichsrelevanz an die Hand gegeben werden.

Zusätzlich wurde in einem Verfahren durch gerichtlichen Beschluss zur Vorgabe gemacht, dass die Sachbearbeiter, die live mithören, täglich neu über den aktuellen Sachstand informiert werden. Dies sollte gewährleisten, dass die Sachbearbeiter in der Lage sind, den in der Wohnung verkehrenden Personenkreis im Hinblick auf die Kernbereichsprognose richtig einzuschätzen:

> *„Aufgrund der verfassungsrechtlichen Vorgaben ist bei der Umsetzung einer richterlichen Überwachungsanordnung mittels geeigneter Maßnahmen organisatorischer Art sicherzustellen, dass im Verlauf der Maßnahme regelmäßige,*

am aktuellen Sachstand orientierte Erhebungsprognosen der jeweils eingesetzten Beamten erfolgen."

In zwei Verfahren wurde die – allerdings nur für zwei bzw. drei Tage angeordnete und auch nur so lang andauernde – Überwachungsmaßnahme durch einen **anwesenden Richter** begleitet, der darüber entschied, wann die Überwachung abzuschalten war.

Der Beschluss hierzu lautete:

„Die Maßnahme wird während der Durchführung in Echtzeit durch zumindest ein Mitglied der Kammer begleitet. Sofern kein Mitglied der Kammer mithört, ist der Vorsitzende unverzüglich von dem dann an Stelle des Gerichts mithörenden Staatsanwalt/polizeilichen Sachbearbeiter oder dessen Vertreter per Handy zur Frage der Unterbrechung des Mithörens und Aufzeichnens der Gespräche zu kontaktieren, wenn Äußerungen fallen, die dem Kernbereich der privaten Lebensführung zuzurechnen sind oder Zweifel auftauchen, ob dieser betroffen sein könnte oder Selbstgespräche geführt werden."

Die Sachbearbeitung hat positive Erfahrungen mit der "physischen" Begleitung der Maßnahme durch ein Gericht gesammelt, da plötzlich auftauchende Fragestellungen sofort gelöst werden konnten und die Verantwortung der Entscheidung über die Kernbereichsrelevanz bei dem anwesenden Richter lag. Dabei wurde zwar keine Situation von dem anwesenden Richter anders eingeschätzt, als dies der Sachbearbeiter getan hätte, aufgrund der großen Unsicherheiten im Umgang mit den gesetzlichen Vorgaben verschaffte jedoch die richterliche Anwesenheit den Sachbearbeitern Sicherheit.

Dies ist gleichwohl auf Einzelfälle und nur auf kurzzeitige Maßnahmen beschränkt, wenn eine besonders kernbereichsproblematische Konstellation zu erwarten ist. Zumeist dürfte die Erreichbarkeit eines Richters ausreichen, um im Zweifel unklare Kernbereichssituationen direkt richterlich klären zu können.

Zwei Indikatoren zur Einschätzung, der Erforderlichkeit einer Echtzeitüberwachung trotz negativer Prognose der Kernbereichsbetroffenheit, wurden im Rahmen der Datenerfassung weder in Fragebögen noch in Expertengesprächen erwähnt, könnten sich aber als sinnvolle Abgrenzungskriterien erweisen: die Anzahl der Kommunizierenden sowie die Thematik

der Kommunikation.[34] Dabei kann zumindest die Anzahl ggf. durch Begleitmaßnahmen (Video, TKÜ etc.) erhoben werden.

Bei einer **Vielzahl anwesender Personen** ist die Kommunikation in der Regel **weniger schützenswert** als bei nur zwei Anwesenden.[35]

Indizcharakter für eine höchstpersönliche Thematik haben zum Beispiel - solange diese nicht von ihm selbst öffentlich preisgegeben werden:

- die Auseinandersetzung des Einzelnen mit sich selbst, seiner Sinnhaftigkeit, seiner Stellung im Leben, seinem Gewissen, seinem Liebesleben, seiner Gefühlswelt, seiner Sexualität, seiner moralischen, religiösen und ethischen Haltung zu den Fragen der Welt und der Gesellschaft.
- seine Auseinandersetzung und Beschäftigung mit Krankheiten, Tod und Rückschlägen in der persönlichen Entwicklung sowie mit der Familie als sozialem Gebilde und den damit verbundenen Problemen.[36]

Dagegen erfordern **Alltagsgespräche** indiziell **kein Live-Mithören**.

In nur einem der untersuchten zehn Verfahren mit Echtzeitüberwachung[37] kam es zu einer nachträglichen Prüfung der Betroffenheit des Kernbereichs privater Lebensgestaltung durch Vorlage bei Gericht nach § 100c Abs. 5 Satz 6 StPO. Hier wurde die Einschätzung des Ermittlungsführers, der Kernbereich sei nicht betroffen, bestätigt, so dass die aufgezeichnete Sequenz nicht gelöscht werden musste.

Die **Probleme beim Live-Mithören** sind ausweislich der Erhebungen des Projekts vielfältig. Stichwortartig können folgende Problemfelder benannt werden:

- schlechte Sprachverständlichkeit, insbesondere Störung bzw. Überlagerung durch Hintergrundgeräusche, was insbesondere bei Sprachen problematisch ist, bei denen

[34] Vgl. hierzu *Warntjen*, Heimliche Zwangsmaßnahmen und der Kernbereich privater Lebensgestaltung, Baden-Baden 2007, S. 88. Weitere von *Warntjen* genannte Kriterien wie beispielsweise die Wahl des Kommunikationsmittels (Telefon!) erscheinen hier weniger geeignet.
[35] Vgl. *Warntjen*, S. 92.
[36] Vgl. *Warntjen*, S. 91.
[37] Bei zwei Verfahren war, wie oben dargestellt, ein Mitglied des Gerichts während der Überwachung anwesend, so dass daher eine weitere gerichtliche Klärung nicht erforderlich war.

es für das inhaltliche Verständnis des Gesagten auf die Betonung und genaue Aussprache ankommt,

- Schwierigkeit der Identifizierung der Sprecher,
- Probleme bei der Feststellung, wer im Objekt anwesend ist,
- erheblicher Personalaufwand für das Einrichten eines Mithörens rund um die Uhr,
- sehr hohe Anforderungen an das Personal wegen der Notwendigkeit, sich über einen langen Zeitraum stark zu konzentrieren,
- technische Störungen,
- Wortprotokolle sind sehr umfangreich und schwierig zu erstellen,
- Zeitverzug durch erforderliche Übersetzung.

Das Live-Mithören stellt die Ermittlungsbehörden insgesamt betrachtet vor **größte Schwierigkeiten**, da es personell sehr aufwendig ist und ggf. zunächst Dolmetscher sowie Sprachtechniker zum Erkennen des Gesprochenen herangezogen werden müssen und die Frage nach dem Zeitpunkt des Wiedereinschaltens nach einer Unterbrechung weitgehend unbeantwortet ist.

Der **Personalbedarf** für das Einrichten eines Schichtbetriebes zur Echtzeitüberwachung liegt nach Erkenntnissen aus Expertengesprächen, die mit den zehn Dienststellen geführt wurden, bei denen eine Echtzeitüberwachung durchgeführt wurde, bei **mindestens zwölf Personen** – vier pro Schicht. In der Regel sind pro Schicht ein Techniker, ein Ermittlungsführer und zwei Sachbearbeiter erforderlich. Bei Überwachung von Kommunikation in fremder Sprache sind darüber hinaus zusätzlich ein bis zwei Dolmetscher – je nach Anzahl der Gesprächsteilnehmer – pro Schicht erforderlich. Für die anschließende Auswertung sowie das Verschriften wird weiteres Personal benötigt.
Bei einem Verfahren wurden nach Auskunft des Ermittlungsführers wegen der Erforderlichkeit einer Echtzeitüberwachung 27 Personen benötigt, nach alter Rechtslage hätte die Maßnahme dagegen seiner Einschätzung nach mit vier Personen realisiert werden können.
Zusätzlich ist zu bedenken, dass externes Personal erst in das Verfahren einzuführen ist, da für die Entscheidung, was relevant ist und was dokumentiert werden muss, detaillierte Kenntnisse des Verfahrens erforderlich sind.

1.7.2.2. Unterbrechen und Wiederzuschalten des Mithörens

Bei Erkennen einer Kernbereichsverletzung ist ein Unterbrechen der Überwachung (s. § 100c Abs. 5 Satz 1 StPO) sowie Löschen des bis zum Erkennen der Verletzung aufgezeichneten Gesprächsabschnitts mit Kernbereichsrelevanz nach den gesetzlichen Vorgaben notwendig.

In gerichtlichen Beschlüssen wurde dies so formuliert:

> *„Die Kammer geht jedoch davon aus, dass die Ermittlungsbehörden dafür Sorge tragen werden, dass insbesondere bei Anwesenheit von Verwandten des Beschuldigten in dieser Wohnung die Überwachung sofort abgebrochen wird, wenn eine Situation eintritt, in der ein unantastbarer Kernbereich privater Lebensgestaltung zum Gesprächsthema gemacht wird."*

oder:

> *„Soweit während der Anwesenheit des Beschuldigten Äußerungen, welche dem Kernbereich der privaten Lebensgestaltung zuzurechnen sind, erfasst und aufgezeichnet werden, werden diese unverzüglich gelöscht. Dazu wird die Maßnahme zeitgleich und dauerhaft durch einen polizeilichen Sachbearbeiter und technisches Personal begleitet. Die Löschung wird dokumentiert."*

Für das rechtliche Verständnis ist es erforderlich, vereinfacht zu erklären, wie das Unterbrechen der Überwachung praktisch funktioniert:
Ein Rekorder zeichnet zur Beweissicherung die eingehenden Tonsignale auf. Das Gerät hat eine Stopptaste zur Unterbrechung sowohl des Audioempfangs als auch der Aufzeichnung. Zu Beginn einer jeden Abhörsequenz trifft der Sachbearbeiter kurzfristig die Entscheidung, ob das empfangene Gesprächssignal aufgezeichnet werden soll. Sofern er sich für eine Aufzeichnung entscheidet, wird eine kurze Inhaltsangabe für das in der Abhörsequenz wahrgenommene Gespräch gefertigt, um den Ablauf zu dokumentieren und die spätere Entscheidung über die Fertigung einer ausführlichen Niederschrift („Audioprotokoll") vorzubereiten. Falls er kernbereichsrelevante Gesprächsinhalte erkennt, stoppt der Sachbearbeiter die Aufnahme und überprüft anschließend – ggf. bei veränderter Personenkonstellation im zu überwachenden Objekt – durch gelegentliches „Hineinhören" die Situation bezüglich einer etwaigen Fortdauer der Kernbereichsrelevanz. Hinsichtlich jeder Abhörsequenz werden der Verlauf einschließlich technischer Daten wie Start- und Endzeit sowie Ordnerbezeichnung, die Entscheidungen über Aufzeichnung und Übersetzung der

Gesprächssequenz sowie eine Kurzinhaltsangabe fortlaufend in einer Tabelle dokumentiert.

In vier von den zehn Verfahren, in denen das Gericht ein Live-Mithören anordnete, war keine Unterbrechung erforderlich. In den sechs Verfahren, in denen die Aufnahme gestoppt wurde, stellte in den überwiegenden Fällen, nämlich in vier Verfahren, die Anbahnung einer intimen Situation bzw. der Besuch einer Prostituierten die Ursache für den Abbruch dar.

Die Feststellung, dass möglicherweise der Kernbereich privater Lebensgestaltung betroffen ist, wurde in den untersuchten zehn Fällen mit Echtzeitüberwachung auf Erkenntnisse aus einer Videoüberwachung des Hauseingangs gestützt, aus den Gesprächsinhalten abgeleitet (Dolmetscher) sowie in einem Fall aufgrund der Hinzuziehung eines Islamwissenschaftlers getroffen, der Angaben dazu machen konnte, wann ein Gebet begann, wodurch Indizien für eine Betroffenheit bzw. Nicht-Betroffenheit im konkreten Einzelfall gewonnen werden können. Eine abschließende Liste von "Instrumentarien" kann angesichts jeweils neu vorgefundener Lebenssachverhalte freilich nicht erstellt werden.

Als ungeklärt gilt ausweislich der analysierten Fragebögen und der geführten Experten-gespräche die Frage, unter welchen Voraussetzungen ein **erneutes Einschalten** der Überwachungstechnologie nach einer Unterbrechung zum Schutz des Kernbereichs privater Lebensgestaltung erlaubt ist.
Als grobe Richtlinie wird derzeit von den Ermittlungsführern angenommen, ein Wieder-einschalten sei nach fünf Minuten Überwachungsunterbrechung wieder zulässig.

Teilweise wurde in den Experteninterviews mehrfach betont, dass ein anlassbezogenes Wiedereinschalten, also ein erneutes Einschalten nach Ablauf der Zeit, die üblicherweise für die private Lebensgestaltung, z.B. bei dem Besuch einer Prostituierten, angesetzt werden muss, erforderlich ist. Hierbei stellt sich jedoch die Frage, wie lange die „übliche“ Zeit für bestimmte Handlungen bzw. Gespräche ist, da die individuelle Disposition des/der Betroffenen durchaus im Einzelfall sehr unterschiedlich ausgestaltet ist und daher nur grobe zeitliche Eingrenzungen vorgenommen werden können. Dies bemisst sich dabei weitgehend an Erfahrungswerten bzw. der Lebenserfahrung.

Das „Hineinhören“ zur Prüfung, ob der Kernbereich privater Lebensgestaltung durch eine weitere Überwachung nicht mehr tangiert werden würde, kann in einigen Fällen, die

eindeutig gelagert sind, sehr kurz sein und ca. 20-40 Sekunden dauern. In anderen Fällen ist es jedoch erforderlich, den Gesamtzusammenhang einer Unterhaltung zu verstehen, so dass hier ein kurzes „Reinhören“ nicht ausreicht, um eine Einschätzung zur Kernbereichsrelevanz weiterer Gespräche oder Situationen abzugeben. Z.B. kann es bei religiösen Themen, insbesondere bei islamistischen Tätergruppierungen im Einzelfall schwierig sein zu beurteilen, ob es sich um einen persönlichen, religiösen Austausch handelt, der eher dem Kernbereich zuzuordnen wäre oder um im Zusammenhang mit der Straftat stehende vermeidlich religiöse Hintergründe.

In zwei Verfahren gab es richterliche Vorgaben dahingehend, dass ein Wiedereinschalten erst zulässig ist, wenn durch andere, weniger eingriffsintensive Maßnahmen sichergestellt werden kann, z.B. eine Observation, dass der Kernbereich privater Lebensgestaltung nicht mehr betroffen ist. Dies hatte zur Folge, dass mittels Videoüberwachung bzw. persönlicher Observation erfasst werden musste, welche Personen wann das Objekt verließen. Die insofern häufig auftauchenden Probleme wurden bereits oben geschildert (etwa Abhängigkeit von Lichtverhältnissen, Verdeckung von Personen durch vorbeifahrende Fahrzeuge, Enttarnung der Maßnahme).

In den sechs Ermittlungsverfahren, in denen es zu einer Unterbrechung des Mithörens kam, ergaben sich unterschiedliche Zeitspannen zum Wiederzuschalten. In einem Fall nahm man ein Wiedereinschalten nach **Lebenserfahrung** vor, d.h. der Ermittlungsführer bestimmte nach seiner individuellen Einschätzung, zu welchem Zeitpunkt wieder zugeschaltet werden konnte. In drei Verfahren waren vom Ermittlungsführer starre Fristen festgesetzt worden, nach deren Ablauf ein Zuschalten erfolgte und die bei zehn Minuten, 15 Minuten bzw. einer Stunde lagen. In einem weiteren Verfahren, dem die richterliche Vorgabe zu Grunde lag, dass nur aufgrund von Observationserkenntnissen wieder zugeschaltet werden durfte, wurde die Maßnahme fortgesetzt, sobald die Zielperson bzw. die Prostituierte das Haus verlassen hatte.

Berichtet wurde ebenfalls von möglichen **Verhaltensweisen durch Tatverdächtige**, die eine Betroffenheit des Kernbereichs eventuell nur vortäuschten, um ein Unterbrechen der Überwachung zu provozieren. Gleichwohl wurde die Maßnahme unterbrochen, so dass retrograd eine mögliche "Umgehungsstrategie" durch die Betroffenen im konkreten Fall nicht verifiziert werden konnte. Allerdings erscheint bei Vorliegen konkreter Anhaltspunkte für eine solche "Umgehungsstrategie" das Abschalten der Aufzeichnung nicht geboten. Dies ist freilich im Einzelfall festzustellen.

Zu dieser Problematik kann h.E. auch die Entscheidung des BVerfG vom 27.02.08, auch wenn sich diese auf die Online-Durchsuchung bezieht, zur Argumentation herangezogen werden. Eine Überwachung ist demnach zulässig, wenn konkrete Anhaltspunkte dafür bestehen, dass Tat- mit Kernbereichsrelevantem vermischt wird, um eine Überwachung zu verhindern.[38] Das BVerfG hat damit den Bedenken Rechnung getragen, dass durch zu formale Vorgaben zum Kernbereichsschutz die Maßnahme von der Täterseite ohne große Schwierigkeiten ad absurdum geführt werden könnte. Um derartige „Präventionsstrategien" seitens der Beschuldigten von vorn herein unmöglich zu machen, wurde den Ermittlungsbehörden ein Beurteilungsspielraum zugestanden, derartige Verdachtsmomente zu erkennen und dann die Überwachung nicht zu unterbrechen. Diese Bedenken gelten gleichermaßen für die Wohnraumüberwachung, so dass h.E. die Argumentation des BVerfG aus der Entscheidung zur Online-Durchsuchung auch auf die Wohnraumüberwachung erstreckt werden kann.

Bei konkreten Anhaltspunkten dafür, dass eine Kernbereichsbetroffenheit von Beschuldigten nur vorgetäuscht wird, um nach Abschalten der Überwachung ungefährdet Tatrelevantes zu besprechen, ist es h.E. zulässig, die Überwachung zunächst fortzusetzen und ggf. eine Entscheidung des Gerichts nach § 100c Abs. 5 Satz 6 StPO über die Fortführung der Maßnahme herbeizuführen.

1.7.2.3. Zulässigkeit der automatisierten Aufnahme

Ergibt die vorgenommene Prognose keine Wahrscheinlichkeit einer Betroffenheit des Kernbereichs privater Lebensgestaltung, ist es zulässig, zunächst sämtliche Gespräche aufzuzeichnen und auf eine Echtzeitüberwachung zu verzichten, sofern **ein Erlangen höchstpersönlicher Inhalte nicht zu erwarten steht**.[39]

Ein richterlicher Beschluss lautete in einem solchen Fall beispielsweise:

> *„Bei der vorliegenden Fallgestaltung sind daher keine Indikatoren dafür gegeben, dass durch die technische Maßnahme der unantastbare Kernbereich der Menschenwürde verletzt werden könnte."*

oder für einen Geschäfts- oder Büroraum:

> *„Es liegen keine Anhaltspunkte dafür vor, dass die Gefahr der Erfassung kernbereichsrelevanter Äußerungen besteht, wie dies bei der Durchführung einer*

[38] BVerfG NJW 2008, 822 (834, Rz. 281).
[39] Vgl. BT-Drs. 15/4533, S. 15 f.

Maßnahme in einer Wohnung zu erwarten wäre. Aus diesem Grund ist es zulässig, die Gespräche automatisch – ohne Echtzeitüberwachung – aufzuzeichnen."

Anordnung des Live-Mithörens

	Häufigkeit	Prozent
ja	10	66,7 %
nein	5	33,3 %
Gesamt	**15**	**100** %

Auf eine Echtzeitüberwachung wurde bei drei von elf Maßnahmen, bei denen es um eine Überwachung von Privatwohnungen ging, verzichtet. In einem dieser drei Verfahren war die Wohnung nicht mehr bewohnt. Außerdem kommunizierten die anwesenden Tatverdächtigen ausschließlich in einer fremden Sprache, was das Einschalten eines Dolmetschers erforderte. Der einzig erreichbare Dolmetscher für den gesprochenen Dialekt war den Beschuldigten jedoch bereits bekannt und hätte aufgrund der besonderen Lage des zu überwachenden Objekts nicht verdeckt in dessen Nähe gelangen können. Ein Empfang der Audiosignale an einem anderen Ort, z.B. auf der Dienststelle, war technisch nicht zu realisieren. In einem anderen Verfahren wurde die Privatwohnung fast ausschließlich für die Planung von Straftaten genutzt und daher eine Echtzeitüberwachung für nicht erforderlich erachtet. Im dritten Verfahren wurde als Begründung für das Absehen von einer Echtzeitüberwachung im richterlichen Beschluss ausgeführt, dass eine zeitnahe Auswertung bis zum Folgetag als ausreichend anzusehen sei.

In einer von drei Maßnahmen in ABG-Räumen sowie einer sonstigen geschützten Räumlichkeit wurde ebenfalls eine Echtzeitüberwachung – ohne Begründung im Beschluss – für nicht erforderlich angesehen.

Bei den Fällen, in denen ein Live-Mithören für nicht notwendig erachtet wurde, erfolgten in zwei Verfahren, welche die Überwachungen von Privatwohnungen betrafen, Vorgaben des Gerichts bezüglich der Auswertung, die spätestens bis zum Folgetag abgeschlossen sein sollte. Eine Maßgabe, die jedoch in einem Verfahren nicht eingehalten werden konnte, da die erfassten Gespräche zunächst ins Deutsche übersetzt werden mussten. Das Gericht verlängerte daraufhin die Frist, so dass die Nichteinhaltung der ursprünglichen Zeitvorgabe letztlich keine Auswirkungen auf das Verfahren hatte. In dem anderen Verfahren konnten die vorgegebenen Fristen nur unter größten Schwierigkeiten eingehalten werden. Dies

beruhte darauf, dass **eine Stunde Aufnahme** von Audiosignalen zwischen zwei und zehn Stunden Auswertung erfordert.

Eine Vorgabe in der richterlichen Anordnung, dem Gericht eine Gesprächsauswertung bis zum Folgetag vorzulegen, ist allenfalls bei kurzzeitigen Überwachungsmaßnahmen – und auch dann nur unter größten Schwierigkeiten – einzuhalten und somit unrealistisch. Wenn eine Vorlage der Gesprächsprotokolle bei Gericht erforderlich ist, sollte als Frist die Vorgabe „unverzüglich nach Fertigstellung“ formuliert werden.

1.7.2.4. Löschen kernbereichsrelevanter Sequenzen

Ein Löschen bestimmter Sequenzen wird erforderlich, wenn automatisiert Kernbereichsrelevantes aufgezeichnet wurde. Ebenfalls notwendig ist bei Echtzeitüberwachung das Löschen von Aufnahmen auf dem Beweisband bis zum Stoppen der Aufnahme (Zeitpunkt des Beginns der Kernbereichsverletzung bis zu deren Wahrnehmung). Sollte ein Gericht im Rahmen der nachträglichen Klärung entscheiden, dass eine aufgezeichnete Sequenz kernbereichsrelevant ist, hat eine Löschung zu erfolgen.

Ein nachträgliches selektives **Löschen** kernbereichsverletzender Sequenzen ist bei Aufzeichnungen, die unter Verwendung von Digitaltechnik hergestellt wurden, nach Auskunft der Experten nur mittels einer besonderen Auswertesoftware und nur durch einen Ingenieur möglich, weshalb dies derzeit weder unmittelbar nach erfolgter Aufzeichnung noch am Einsatzort zu realisieren ist.

Im Bericht des UA IuK[40] wird darauf hingewiesen, dass technisch eine durchgängig digitale Aufzeichnung angestrebt wird. Die Aufzeichnung des Audiosignals erfolgt dann nach den gesetzlichen Vorgaben, die ein Stoppen der Aufnahme bei erkennbarer Verletzung des Kernbereichs privater Lebensgestaltung vorsehen und die ferner ein Wiederstarten der Aufzeichnung gestatten, wenn keine Verletzung mehr droht.
Die Anschaffung neuer Techniksysteme nach dem Beschluss der KOMGÜT-Arbeitsgruppe[41] hat sich jedoch als sehr zeitaufwändig erwiesen, da die Anforderungen an das System zunächst festgelegt und beschrieben werden mussten.

[40] Bericht „Auswirkungen des BVerfG-Urteils zur akustischen Wohnraumüberwachung; Technische Rahmenbedingungen für die Modifikation oder Neubeschaffung/Neuentwicklung von Systemen zur Langzeitaufzeichnung“, Stand: 10.01.2006 der Kommission „IuK-Grundlagen der Überwachungstechnik“.

[41] Derzeit (März 2008) verfügen nicht alle Länder über die oben beschriebenen Systeme.

1.8. Einsatz von Sprachmittlern

Die Auswertung der Fragebögen sowie Expertengespräche hat ergeben, dass **Sprachmittler** aus ihrer Übersetzungstätigkeit bei Telekommunikationsüberwachungen in der Regel eine sehr gute Sprachqualität gewohnt sind, da die meist bekannten Teilnehmer direkt ins Mikrofon sprechen. Diese Qualität ist bei einer Wohnraumüberwachung aufgrund

- des räumlichen Klangs,
- der Distanz zum Mikrofon und
- der Nebengeräusche, z.B. von vorbeifahrenden Fahrzeugen, nicht zu erzielen.

Hinzu kommen folgende Probleme:

- Schwierigkeiten, die Stimmen einzelnen Personen zuzuordnen,
- Überlagerungen der gesprochenen Worte und Sätze aufgrund gleichzeitigen Sprechens mehrerer Gesprächsteilnehmer.

Der Dolmetscher muss sich daher eine Übertragung aus einem Wohnraum in der Regel mehrmals anhören, vor allem, wenn nur schwer zu verstehende Dialekte gesprochen werden. Das bedeutet bei einem Live-Mithören, dass das aktuell Gesprochene in diesem Moment verpasst wird. Dadurch ist in weiterer Konsequenz auch ein verspätetes **Erkennen einer Kernbereichsverletzung** möglich. Darüber hinaus kann es aufgrund der Übersetzung zu Fehlinterpretationen kommen, die eine Aussage über eine Kernbereichsbetroffenheit nicht zulassen. Im Übrigen lässt oftmals ein Mangel an geeigneten Dolmetschern ein längeres Live-Mithören nicht zu.

Hierzu ein Auszug aus einem Beschluss:

> *„Die Übersetzung der relevanten Wohnraumgespräche erwies sich schon aufgrund der – bei einer TKÜ weithin unbekannten – akustischen Verständigungsschwierigkeiten (etwa aufgrund von vielfältigen Störgeräuschen, z.B. des nahezu immer mitlaufenden Fernsehgerätes) deutlich zeitaufwändiger als bei Telefongesprächen (ca. 1 Stunde Übersetzungsarbeit für etwa eine Gesprächsminute).“*

Da der Einsatz von Sprachmittlern bei Wohnraumüberwachungsmaßnahmen häufig erforderlich ist – in den betrachteten Verfahren in der Hälfte der Fälle –, wiegen diese Probleme besonders schwer.
In vier von sieben Verfahren mit Sprachmittlern wurde daher auf ein Live-Mithören verzichtet. Eine Begründung hierfür lautete:

> *„Das angestrebte Ziel der Maßnahme würde erheblich gefährdet werden, wenn die Dolmetscherin mit Beamten des MEK die Aufzeichnung vor Ort abhören würde. Die Dolmetscherin kann in dem leerstehenden Haus nicht zwei Wochen rund um die Uhr untergebracht werden. Ein Erscheinen auf Abruf vor Ort scheidet aus, da es sich bei der Straße um eine sehr schmale, ruhige Straße handelt. Alle Beschuldigten kennen die Dolmetscherin als Dolmetscherin der Polizei. Das Risiko wäre hoch, dass die Dolmetscherin von einem der Beschuldigten gesehen und erkannt würde."*

1.9. Verfahrensrelevante Erkenntnisse sowie deren Verwertung im gerichtlichen Verfahren

In 10 der 14 analysierten Verfahren führte die akustische Wohnraumüberwachung zur Aufklärung des Sachverhalts. Bei vier Fällen erbrachte die Maßnahme kein Ergebnis, und zwar überwiegend deshalb, weil keine verfahrensrelevanten Gespräche geführt wurden.

Bei einem Verfahren konnten durch die Maßnahme nach § 100c StPO Erkenntnisse für ein anderes Verfahren nach §§ 129a, b StGB erlangt und in Anbetracht des Vorliegens einer Katalogtat nach § 100c StPO unproblematisch verwertet werden (Zufallsfund).

Von den zehn Verfahren, die verwertbare Ergebnisse erbrachten, wurde ein Verfahren eingestellt, und zwar nicht zuletzt deshalb, weil die Erkenntnisse aus der Wohnraumüberwachung **zur Entlastung** der Beschuldigten beitrugen.

In einem Verfahren war die Überwachung nach Aussage des Ermittlungsführers sehr hilfreich für den Fortgang der Ermittlungen. Ein weiterer Prozess endete mit einer Verfahrensabsprache („Deal") vor Gericht, **ohne** dass es zu einer **Verwertung** der Erkenntnisse aus der Wohnraumüberwachung kam. In zwei Verfahren wurde die Wohnraumüberwachung zwar in den jeweiligen Urteilen erwähnt, die Verurteilung der Angeklagten beruhte aber ausschließlich auf anderen Beweismitteln.

In einem Prozess vor dem OLG Düsseldorf (Urteil des 6. Strafsenats vom 05.12.07) waren Erkenntnisse aus einer Wohnraumüberwachung das **Hauptbeweismittel**. Das Gericht setzte sich deshalb umfänglich mit der Zulässigkeit der Einführung der Erkenntnisse der Wohnraumüberwachung in das Verfahren auseinander. Dabei bescheinigte der Vorsitzende Richter den ermittelnden Kriminalbeamten ausdrücklich ein besonders hohes Maß an rechtlicher Aufmerksamkeit und Sensibilität, namentlich in Bezug auf die penible Beachtung der Vorgaben des BVerfG.

Vier Fälle waren zum Zeitpunkt der Abfassung dieses Berichts noch nicht abgeschlossen, so dass zum derzeitigen Zeitpunkt keine Aussage über eine Verwendung der erlangten Erkenntnisse getroffen werden kann.

Hinsichtlich der Beweiswürdigung ist zu beachten, dass der **Beweiswert** einer Aufzeichnung, bei der Sequenzen gelöscht wurden, fraglich sein kann, da in einem solchen Fall eine Veränderung der Originalaufnahme erfolgt ist und somit Manipulationen als nicht gänzlich ausgeschlossen erscheinen. Die Problematik gilt im Übrigen gleichermaßen bei der Regelung der TKÜ (s. § 100a IV StPO).

1.10. Alternativmaßnahmen zu Wohnraumüberwachungen nach § 100c StPO

Trotz der skizzierten Schwierigkeiten bei der Realisierung von Wohnraumüberwachungen konnte ein **Ausweichen auf Alternativmaßnahmen** nicht festgestellt werden. Die Zahl der Überwachung von Fahrzeugen oder der akustischen Überwachungen außerhalb von Gebäuden hat zwar zugenommen, dies ist aber nach Erkenntnissen aus den Expertengesprächen nicht auf erwartete Schwierigkeiten mit einer Wohnraumüberwachung zurückzuführen, sondern auf eine Verbesserung der Technik und der damit erzielbaren Ergebnisse. Zudem ist die Wohnraumüberwachung aufgrund des Erfordernisses der Subsidiarität ohnehin „ultima ratio“. Dies bedeutet, dass weniger eingriffsintensive Alternativmaßnahmen in der Regel bereits vor einer Wohnraumüberwachung ergriffen wurden, aber keinen Ermittlungserfolg erbrachten, so dass derartige Maßnahmen dann, wenn über eine Wohnraumüberwachung nachgedacht wird, nicht mehr als mögliche Alternativmaßnahmen in Betracht gezogen werden können.

Nach Einschätzung der betroffenen Dienststellen ist die Wohnraumüberwachung im linksextremistischen Bereich regelmäßig der einzige Erfolg versprechende Ermittlungsansatz, da die üblichen verdeckten Ermittlungsmaßnahmen TKÜ und Observation nur

Bewegungsbilder bzw. Informationen zu Kontaktpersonen liefern, nicht jedoch Hinweise, die zur Überführung von Tatverdächtigen geeignet sind.

1.11. Zentrale Schlussfolgerungen

Die gewonnenen Erkenntnisse lassen folgende zentrale Bewertung zu:

1.11.1. Gründe für den Rückgang der Anzahl der Maßnahmen nach § 100c StPO

Der Vorsitzende Richter des Staatsschutzsenates des OLG Düsseldorf formulierte es in seinem Vorwort zur mündlichen Urteilsbegründung in einem Verfahren wegen der Mitgliedschaft bzw. Unterstützung einer terroristischen Vereinigung am 05.12.07 wie folgt:

> *„Die gesetzliche Neuregelung ist in der Praxis nur mit überaus großen Hindernissen und Beschwernissen durchführbar und stellt bei der Ermittlung in Fällen schwerster Kriminalität ein eher stumpfes Schwert dar.“*

Aus den dargestellten Gründen sind die Vorgaben durch das BVerfG durch das Urteil zur Wohnraumüberwachung und die hieraus resultierenden Vorgaben der gesetzlichen Regelungen (§§ 100c ff. StPO) eine Erschwernis für die polizeiliche Praxis (technisch, taktisch, personell).

Es ist im Rahmen dieses Projekts nachgewiesen, dass der Rückgang der Zahl der Wohnraumüberwachungen seit 2004/2005 auch auf die Unsicherheit in den sachbearbeitenden Dienststellen schon in der Prüfungsphase, ob eine solche Maßnahme unter Einhaltung der neuen Vorgaben realisiert werden kann, zurück zu führen ist. Die überwiegende Antwort auf die Frage der Gründe für den Rückgang war, dass die Maßnahme nicht mehr praktikabel bzw. handhabbar sei. Hier besteht erheblicher Aufklärungsbedarf, zu dessen Behebung dieser Abschlussbericht beitragen kann. Die oftmals vorzufindende Skepsis der Dienststellen gegenüber dem Instrument der WRÜ ist angesichts der hohen gesetzlichen Hürden und vagen Vorgaben des BVerfG zum Kernbereichsschutz nicht nur nachvollziehbar sondern auch angebracht, zudem "blockiert" sie die Maßnahme der Wohnraumüberwachung oftmals noch zusätzlich und von vornherein.

Dagegen benannten Dienststellen aus zwei Bundesländern als Ursache für den Rückgang der Zahl der Wohnraumüberwachungen die offenbar kategorische Weigerung der

Staatsanwaltschaften bzw. Gerichte, Beschlüsse nach § 100c StPO zu beantragen bzw. zu erlassen, so dass in diesen Ländern trotz des entsprechenden polizeilichen Willens und erkannter Notwendigkeit keine akustischen Wohnraumüberwachungen erfolgten. In zwei weiteren Ländern wurden grundsätzliche Bedenken einzelner Staatsanwaltschaften bzw. Gerichte gegen die Zulässigkeit von Maßnahmen nach § 100c StPO geschildert. Eine generelle landesweite Ablehnung gab es dort aber jeweils nicht.

Lediglich in einem Fall wurde als Grund für den Rückgang von Wohnraumüberwachungsmaßnahmen der **veränderte Straftatenkatalog** angeführt, der durch das Heraufsetzen der Schwelle Maßnahmen bei Delikten ausschließe, bei denen man eine Wohnraumüberwachung eigentlich für notwendig erachtet hätte.

Nur in einem der betrachteten 15 Fälle scheiterte eine Überwachung aus technischen Gründen, weil der Einbau der Technik nicht gelang. In einem weiteren Verfahren wurde die laufende Überwachung abgebrochen, da zu viele Störgeräusche auftraten.

Überwiegend wird in der Polizeipraxis die Einschätzung, die Wohnraumüberwachung sei „tot“, nicht geteilt, allerdings anerkannt, dass die Begründung und Durchführung der Maßnahme erheblich erschwert oder gar vereitelt wird, insbesondere hinsichtlich des Kernbereichsschutzes und der Problematik des "live-Mithörens"(s. 1.11.2).

Die Zahl der Wohnraumüberwachungsmaßnahmen ist derzeit konstant rückläufig. Dies wurde damit begründet, dass die rückläufige Zahl neben den vorgenannten Problemen auch aufgrund einer reservierte Haltung der Sachbearbeitung gegenüber der neuen gesetzlichen Vorgaben aufgrund häufig erheblicher Unklarheiten und Unsicherheiten, also auch schon in der Phase des "Erwägens" der Anregung einer WRÜ, bestehe. Mit zunehmenden Erfahrungswerten und Handlungssicherheit im Umgang mit dem Ermittlungsinstrument könnten die Fallzahlen perspektivisch langsam ansteigen.

1.11.2. Weitere zentrale Erkenntnisse und deren Bewertung

Auch wenn die Fallzahlen **konstant rückläufig** sind, werden nach wie vor Maßnahmen nach §§ 100c ff. StPO durchgeführt. Die Wohnraumüberwachung war und ist aufgrund der hohen Eingriffsintensität und des Subsidiaritätserfordernisses immer schon **ultima ratio**. Der hohe Personalaufwand sowie hohe taktische Risiken verdeckter Maßnahmen werden die Wohnraumüberwachung nie zu einer „Standardmaßnahme“ werden lassen. Vor allem

kurzzeitige Überwachungen (bis zu drei Tagen) sowie Überwachungen von Räumlichkeiten, bei denen eine Prognose ergibt, dass eine Echtzeitüberwachung nicht geboten ist, erscheinen weiterhin realisierbar. Dagegen sind Überwachungen über einen längeren Zeitraum mit Live-Mithören sowie Gesprächen, die in fremder Sprache geführt werden, nur ausgesprochen schwierig zu realisieren.

Die von der Polizeipraxis unmittelbar im Anschluss an das Urteil des BVerfG zur akustischen Wohnraumüberwachung befürchteten Probleme bei der Handhabung der Maßnahme haben sich jedoch weitgehend bewahrheitet. Ein **wesentliches Problem** bereitet in der polizeilichen Praxis das Erfordernis des **Live-Mithörens**.

Oftmals ist **zu wenig Personal** für die Durchführung einer solchen Maßnahme vorhanden, da üblicherweise im Laufe von Ermittlungsverfahren immer mehr Personal abgezogen wird und Wohnraumüberwachungen häufig erst in einem relativ späten Stadium der Ermittlungen ergriffen werden. Die Personalkapazitäten für akustische Wohnraumüberwachungen sind oftmals nur im Bereich des **Staatsschutzes** ausreichend, um eine Maßnahme nach § 100c StPO realisieren zu können, was sich auch in den Katalogtaten – sechs von 15 Verfahren nach §§ 129, 129a, b StGB als Anlasstat – widerspiegelt.

Das **Erkennen kernbereichsrelevanter Situationen** stellt die mithörenden Sachbearbeiter vor erhebliche Schwierigkeiten. Zum einen ist das Erkennen des Gesprächsinhalts generell durch die Verwendung kryptierter Sprache und bei Gesprächen in fremder Sprache problematisch. Zum anderen bereiten die schlechte Sprachverständlichkeit und die partielle Unmöglichkeit, Sprecher zu identifizieren, Probleme. Nicht zuletzt ergeben sich Schwierigkeiten dadurch, dass Wohnraumüberwachungen sehr hohe Anforderungen an das Personal stellen, da sie das Erfordernis einer starken Konzentration über einen langen Zeitraum hinweg mit sich bringen.

Schon bei der **Vorbereitung** der Wohnraumüberwachung zeigen sich die Auswirkungen des Erfordernisses des Kernbereichsschutzes. So ist die in der Regel für unbedingt erforderlich erachtete Videoüberwachung im Außenbereich zum Erkennen von Personen häufig technisch nur schwer auszuführen.

Auffällig sind zahlreiche richterliche Vorgaben, die gewährleisten sollen, dass die Maßnahme **Verhältnismäßigkeitserwägungen** genügt, wie beispielsweise:

- eine nur kurze Laufzeit des Beschlusses (z.B. drei Tage),

- die Anordnung einer Echtzeitüberwachung in Arbeits- und Geschäftsräumen,
- die Anordnung der Anwesenheit eines Richters bei der Überwachung sowie
- die Erteilung einer Erlaubnis für ein erneutes Einschalten nach einer Unterbrechung mit der Maßgabe, dass eine solches Wiedereinschalten nur aufgrund anderweitig erlangter Erkenntnisse statthaft sei.

Aber auch der polizeiliche Umgang mit § 100c StPO zeigt deutlich, dass der Grundsatz der Verhältnismäßigkeit gewahrt wird. Beispielsweise war die Dauer der tatsächlichen Überwachungen, soweit im Rahmen des Projekts Daten erhoben wurden, in aller Regel deutlich kürzer, als der im richterlichen Beschluss genannte Zeitraum. Dritte, die nach § 100c Abs. 2 Satz 3 StPO nur dann betroffen sein dürfen, wenn dies unvermeidbar ist, wurden nur in sehr geringem Maß überwacht. Die überwiegende Anzahl aller Betroffenen wurde über die Durchführung der Maßnahmen benachrichtigt. Der Umgang mit § 100c StPO ist mithin **insgesamt** als in hohem Maß **verantwortungsbewusst** zu bezeichnen.[42]

In Anbetracht der hohen Anforderungen an die Technik, die ein sofortiges Unterbrechen sowie nachträgliches Löschen zulassen muss, wurde von mehreren Dienststellen die Einrichtung eines bzw. mehrerer **Kompetenzzentren** für Wohnraumüberwachungstechnik **gefordert**, die die nötige Technik vorhalten und installieren sowie die Sachbearbeiter in die Bedienung einweisen könnten.

1.11.3. Gesetzgeberischer Handlungsbedarf

Nachfolgend werden die wesentlichen, in den Experteninterviews vorgebrachten Forderungen dargestellt:

- Ein Lösungsansatz zur Reduzierung der Probleme bei Wohnraumüberwachungen ist das so genannte **Richterband**, das zum einen den erforderlichen Schutz des Kernbereichs gewährleisten und zum anderen die Handhabung von § 100c StPO deutlich erleichtern könnte. Das Richterband ist eine durchgängige Aufzeichnung unter Einschluss kernbereichsrelevanter Gespräche, die auf dem Beweisband nicht aufgezeichnet bzw. gelöscht wurden. Es steht lediglich dem Gericht zur Verfügung. Der Richter kann dann entscheiden, ob bestimmte Sequenzen, die nur auf dem

[42] Zu diesem Ergebnis kam ebenfalls die rechtstatsächliche Untersuchung im Auftrag des Bundesministeriums der Justiz von *Meyer-Wieck*, Der große Lauschangriff – Eine empirische Untersuchung zu Anwendung und Folgen des § 100c Abs. 1 Nr. 3 StPO, Berlin 2005, wenn auch zur alten Rechtslage.

Richterband vorhanden sind, verwertet werden dürfen. Der Einsatz des Richterbandes alleine würde aber **ein Live-Mithören nicht entbehrlich machen**, da die Ermittlungsbehörden weiterhin bei kernbereichsrelevanten Äußerungen ihre Aufzeichnung auf dem Beweisband abschalten müssten. Jedoch könnte der Vorwurf, selektiv und vor allem entlastendes Material nicht aufgezeichnet bzw. gelöscht zu haben, mit dem Richterband entkräftet werden. Darüber hinaus könnten möglicherweise entlastende Äußerungen, die nicht mitgehört und nicht auf dem Beweisband aufgezeichnet wurden, weil das Live-Mithören und die Aufzeichnung auf dem Beweisband aus Kernbereichsschutzgründen beendet oder unterbrochen worden war, in das Verfahren eingebracht werden. Der forensische Beweiswert und die Authentizität einer Richterbandaufnahme wären höher als dies bei einem Band mit unterbrochener Aufzeichnung der Fall ist.

Bei der Novellierung von § 100c StPO wurde die Einführung eines Richterbandes jedoch abgelehnt.[43] Im rheinland-pfälzischen Polizeigesetz ist das Richterband hingegen für den Bereich präventiver Wohnraumüberwachungen vorgesehen.[44] Der Verfassungsgerichtshof von Rheinland-Pfalz hat diese Regelung für verfassungsgemäß erachtet.[45] Auch wenn ein Rückschluss von der Verfassungsmäßigkeit einer präventiven Regelung auf die Verfassungsmäßigkeit einer vergleichbaren repressiven Regelung nicht ohne Weiteres möglich ist, so kommt dem Verdikt des rheinland-pfälzischen Verfassungsgerichtshofs doch eine gewisse Indizwirkung zu.

Inwieweit das vom BVerfG in der Entscheidung zur Online-Durchsuchung[46] entwickelte **zweistufige Kernbereichsschutzkonzept** auf die Wohnraumüberwachung übertragen werden kann, ist durchaus zu diskutieren. Zumindest bei den dargestellten Problemen im Zusammenhang mit fremdsprachigen Gesprächen erscheint nach Ansicht des Projektteams eine vergleichbare Ausgangslage gegeben zu sein.

- Eine Normierung der **Verpflichtung Dritter zur Zusammenarbeit** mit den Strafverfolgungsbehörden, wie dies bei § 100b Abs. 3 StPO der Fall ist, würde für den Bereich des § 100c StPO größere Rechtssicherheit schaffen. Die gesetzliche

[43] Vgl. BT-Drs. 15/5486.
[44] § 29 Abs. 8 POG.
[45] Vgl. MMR 2007, 578 ff. Ebenso *Krey*, Festschrift für Schwind, Heidelberg 2006, S. 725 (735) sowie *Perne*, DVBl. 2006, 1486 (1488 ff.).
[46] Vgl. BVerfG NJW 2008, 822 (833 f.).

Normierung einer solchen Forderung ist aus hiesiger Sicht jedoch schwierig, weshalb eine Untermauerung mit Rechtstatsachen nötig wäre.

- Um eine Identifizierung der im zu überwachenden Objekt anwesenden Personen zu erleichtern und ein zeitlich schnelleres Wiederzuschalten nach einer Unterbrechung aus Gründen des Kernbereichsschutzes zu ermöglichen, wäre die Zulässigkeit einer begleitenden repressiven Videoüberwachung **im Nahbereich von Wohnungen** - z.B. im Hausflur eines Mehrfamilienhauses - sehr hilfreich. Im Vergleich zur derzeit ebenfalls unzulässigen Videografie im Objekt - z.B. der Privatwohnung - selbst wäre eine Nahbereichsüberwachung eine weniger eingriffsintensive Maßnahme. Hintergrund dieser Problematik ist die weite Auslegung des Wohnungsbegriffs durch das BVerfG.

1.12. Checkliste für Maßnahmen gemäß § 100c StPO

Nachfolgende Checkliste[47] richtet sich an Sachbearbeiter, die eine Wohnraumüberwachung in einem Ermittlungsverfahren in Betracht ziehen. Ziel ist es, eine Hilfestellung bei der Abschätzung zu geben, ob sich die Maßnahme realisieren lässt.

1. Anlasstaten

- bestimmte, in § 100c Abs. 2 StPO abschließend aufgezählte, schwerwiegende Straftaten aus dem StGB, dem Asylverfahrensgesetz, dem Aufenthaltsgesetz, dem Betäubungsmittelgesetz, dem Gesetz über die Kontrolle von Kriegswaffen, dem Völkerstrafgesetzbuch sowie aus dem Waffengesetz
- Die Tat **muss auch im konkreten Einzelfall besonders schwer wiegen**.

2. Begriff der **Wohnung**

- **Privatwohnungen** sind alle abgegrenzten Räume, die der allgemeinen Zugänglichkeit durch eine räumliche Abschottung entzogen und zur Stätte privaten Lebens und Wirkens gemacht worden sind.
  (z.B. Wohnräume jeder Art, auch Zweitwohnungen, Untermietwohnungen, Wochenendhäuser, Miethäuser, Altersheime, Studentenwohnheime, einschließlich der Nebenräume wie Böden, aber auch Hotelzimmer, Hausboote, Zelte sowie Krankenzimmer und Zubehörflächen, die in erkennbarem Zusammenhang mit Wohnraum stehen, wie Keller, Hof oder Garten, sind vom Wohnungsschutz umfasst.)
- **Arbeits-, Betriebs- und Geschäftsräume** (ABG-Räume) sind Räume, die grundsätzlich der Öffentlichkeit zugänglich sind, aber in den Zeitspannen, in denen sie gerade nicht öffentlich zugänglich sind, als schutzwürdig erachtet werden.
  (z.B. Läden, Kanzlei- und Praxisräume, Büroräume, Verkaufsräume, Gaststätten, Imbissräume, Werkstätten, Montagehallen, Scheunen, Stallungen oder Lagerhallen.)
- **Sonstige geschützte Räume** sind z.B. Kirchen und Klöster, abgeschlossene Höfe, Schlafwagenabteile, Campingbusse, die Fahrerkabine eines Lkw, Vereinshäuser oder Clubräume.
- **Keine Wohnung** (Zulässigkeit einer Überwachung nach § 100f StPO) sind: ABG-Räume während der Öffnungszeiten, Besucherräume in Untersuchungsgefängnissen, Haftzellen, Unterkunftsräume für Soldaten oder Polizeibeamte sowie Pkw.
- **Wohnungsinhaber** ist der unmittelbare Besitzer, also z.B. der Mieter, Untermieter, Gast im Hotel, Mitbesitzer (z.B. bei einer Lebensgemeinschaft), der Besitzdiener (z.B. Internatsschüler, Obdachlose im Obdachlosenheim, Kranke im Krankenzimmer) oder

[47] Die Übersicht orientiert sich an einem vom BKA erstellten Bericht „Rechtliche, kriminaltaktische und praktische Auswirkungen des Urteils des BVerfG zur akustischen Wohnraumüberwachung (Stand 03.06.2004), dem als Anlage 2 eine Checkliste beigefügt war, deren Gedanken aufgegriffen und durch die Projekterkenntnisse angereichert wurden.

bei Geschäftsräumen der Unternehmer.

3. Subsidiarität

Andere Ermittlungsmaßnahmen mit geringerer Eingriffstiefe müssen zunächst eingesetzt worden sein bzw. ihre Anwendung darf nicht Erfolg versprechend sein. Die Wohnraumüberwachung ist **ultima ratio**.

4. Vorbereitende Maßnahmen

- Bis zu **vier Wochen sind** für eine optimale Vorbereitung einzuplanen.
- **Frühzeitige Einbindung** ElAu/MEK, ggf. StA und Gericht. Mit allen Beteiligten ist vorab zu klären, was technisch überhaupt möglich ist, damit keine Beschlüsse erlassen werden, die nicht zu realisieren sind.
- Ein **Betreten** des zu überwachenden Objekts ist nur mit richterlichem Beschluss zulässig. Von dem § 100c StPO-Beschluss sind alle erforderlichen Maßnahmen zum Einbau- und Ausbau der Technik umfasst.
- **Prognoseentscheidung bzgl. der Kernbereichsrelevanz**

  Die akustische Wohnraumüberwachung muss unterbleiben, wenn Anhaltpunkte dafür bestehen, dass in den Kernbereich privater Lebensgestaltung (z.B. bei Gesprächen unter Vertrauenspersonen) eingegriffen wird. Vor der Überwachung ist deshalb eine Prognose hinsichtlich eines möglichen Eingriffs in den Kernbereich privater Lebensgestaltung zu erstellen.

  Indikatoren ergeben sich aus:

  a) der **Art der zu überwachenden Räume**

  ABG-Räume sind weniger geschützt als Privatwohnungen (Indizien für Räume zu Wohnzwecken: Privatbereich, Abgeschlossenheit, Öffentlichkeitsausschluss). Bei der Beurteilung dürfte es - auch technisch - schwierig oder gar unmöglich sein, zwischen einzelnen Räumen eines Objekts zu unterscheiden.

  b) dem **Personenkreis**, der sich in der zu überwachenden Wohnung aufhält

  Bei Anwesenheit von Personen, die dem höchstpersönlichen vertraulichen Umfeld zuzurechnen sind (Eheleute, Verwandte, enge Freunde, Berater), ist verstärkt zu prüfen, ob der Kernbereich betroffen ist.

  Bestehen vor der Maßnahme Anhaltspunkte für eine Tatbeteiligung der Personen des Vertrauens, ist die akustische Wohnraumüberwachung allerdings grundsätzlich (d.h. auf der Anordnungsebene) zulässig. soweit tatrelevante Gespräche zu erwarten sind.

  c) dem zu **erwartenden Gesprächsinhalt**

  Bestehen vor der Maßnahme Anhaltspunkte dafür, dass die zu erwartenden Gespräche einen Bezug zu Straftaten aufweisen, ist die akustische Wohnraumüberwachung zulässig.
- Für die Prognoseerstellung und Vorbereitung der Wohnraumüberwachung sind **Aufklärungsmaßnahmen** erforderlich:

- Auswertung der bisherigen Ermittlungsakten und polizeilicher sowie externer Dateien und Sammlungen
- Fortlaufende Auswertung von Erkenntnissen bereits laufender operativer Aufklärungsmaßnahmen zum Erkennen der Nutzung der Wohnung und der sich in ihr aufhaltenden Personen, z.B. TKÜ, Observation, VE-/VP-Einsatz
- Zentrales Problem hierbei: Eine Videoüberwachung aller Zugänge zum Objekt ist so zu realisieren, dass Personen bei jeglichen Lichtverhältnissen erkannt werden können; generelles Problem des Bekanntwerdens der Videoüberwachung.

- Ist eine **Mitwirkung Dritter** (z.B. Schlüsselhersteller) erforderlich, sollte bei Beschlussbeantragung eine gesonderte Ausfertigung des Beschlusses zur Vorlage bei dem betroffenen Dritten erbeten werden. Inhalt: Gericht, Datum, Aktenzeichen, Rechtsgrundlage, Beschuldigter sowie gegebenenfalls die Verpflichtung des Dritten zur Verschwiegenheit.

5. Durchführung von Maßnahmen während der Überwachung

- ggf. Übertragung der Maßnahme auf eine Fachdienststelle
- erforderliche Observationsmaßnahmen
- permanenter Abgleich der Kernbereichsprognose
- **Live-Mithören** zum Erkennen etwaiger Kernbereichsrelevanz, wenn trotz negativer Prognose eine gewisse Wahrscheinlichkeit von Kernbereichsverletzungen besteht
  - Erstellen von „Handlungsanweisungen“ durch die Ermittlungsführung für alle mit der Realisierung der Echtzeitüberwachung betrauten Personen
  - Der Personalaufwand für eine Echtzeitüberwachung beträgt ca. zwölf Personen im 4-Schicht-Betrieb. Ggf. ist der Einsatz von Dolmetschern zur simultanen Übersetzung erforderlich.
  - Unterbrechen der Maßnahme bei erkannter Kernbereichsrelevanz. Als kernbereichsrelevant können, soweit sie nicht gleichzeitig einen Tatbezug aufweisen, erachtet werden:
    - Ausdrucksformen der Sexualität,
    - Selbstgespräche,
    - individuelle Gebete/Gespräche über religiöse Themen

    Dagegen sind Alltagsgespräche als **nicht kernbereichsrelevan**t anzusehen. Je mehr Personen an der Kommunikation teilnehmen, umso eher ist von Kernbereichsirrelevanz auszugehen. Letztlich ist aber eine **einzelfallbezogene Bewertung** der jeweiligen Situation erforderlich.
  - Ausschluss von Manipulationen durch Tatverdächtige, die eine Betroffenheit des Kernbereichs nur vortäuschen, um ein Unterbrechen der Überwachung zu provozieren.
  - Ggf. muss eine nachträgliche Klärung der Kernbereichsrelevanz nach § 100c Abs. 5 Satz 6 StPO erfolgen.
  - Stichprobenartiges erneutes Mithören zum Erkennen oder Ausschluss der weiteren

Kernbereichsrelevanz nach Lebenserfahrung und ggf. vorheriger Klärung mit der Staatsanwaltschaft/dem Gericht, wann wieder zugeschaltet werden darf.

- Ist ein Erlangen höchstpersönlicher Inhalte nicht zu erwarten, ist eine **automatisierte Aufzeichnung** zulässig. Richterliche Vorgaben, dem Gericht z.B. bereits bis zum Folgetag Gesprächsabschriften vorzulegen, sind oftmals schwierig zu realisieren. Einer so engen Zeitvorgabe sollte daher vor der Beschlussfassung entgegengewirkt werden.

- Genaue und im Nachhinein nicht veränderbare Dokumentation der Abschaltung und Wiedereinschaltung der Maßnahme.
- Löschung kernbereichsrelevanter Daten und Dokumentation der Löschung.

6. Benachrichtigung Betroffener nach § 101 StPO

- Zu benachrichtigen sind:
  - Beschuldigte,
  - Inhaber und Bewohner der Wohnung,
  - sonstige überwachte (auch zufällig in der Wohnung gewesene) Personen
- Die Benachrichtigung unterbleibt, wenn ihr überwiegend schutzwürdige Belange einer betroffenen Person entgegenstehen.
- Die Benachrichtigung der Betroffenen ist gegen eine mit ihr u.U. einhergehende Vertiefung des Grundrechtseingriffs abzuwägen – dabei ist auch zu berücksichtigen, welchen Aufwand die Feststellung der Identität erfordert und welche Beeinträchtigung der Betroffenen damit verbunden sein könnte.
- Identifizierung der Betroffenen und Weiterleitung der Personalien an die Staatsanwaltschaft

7. Weiterverwendung der Daten

- Kennzeichnung der Daten als Erkenntnisse einer Wohnraumüberwachung durch Datenübermittler und Datenempfänger
- Verwertbarkeit von Zufallsfunden nur bei Katalogtaten

8. Datenvernichtung

- Sperren von erhobenen Daten bis zur Unterrichtung
- Löschung aller Daten, wenn sichergestellt ist, dass die Daten für eine gerichtliche Überprüfung nicht mehr benötigt werden

2. Themenkomplex: Bildung terroristischer Vereinigungen, § 129a Abs. 2 StGB

Durch die Neuregelung von § 129a Abs. 2 StGB Ende 2003[48] wurde die Norm grundlegend umgestaltet und die Gründung einer neuen Kategorie terroristischer Vereinigungen sowie die Beteiligung an einer solchen Organisation unter Strafe gestellt. Ziel der Novellierung, die auf dem Gesetz zur Umsetzung des Rahmenbeschlusses des Rates vom 13. Juni 2002 zur Terrorismusbekämpfung und zur Änderung anderer Gesetze beruhte, war es, europaweit eine effektivere Terrorismusbekämpfung zu ermöglichen.

Im Vergleich zu § 129a Abs. 1 StGB a. F. wurde der Straftatenkatalog erweitert.[49] Allerdings müssen die ergänzten Katalogtaten objektive und subjektive **Qualifikationsvoraussetzungen** erfüllen:

- Sie müssen **objektiv** geeignet sein, durch die Art ihrer Begehung oder ihre Auswirkungen einen Staat oder eine internationale Organisation ernsthaft zu schädigen.
- Im **subjektiven Tatbestand** ist ein qualifizierter Vorsatz, die so genannte terroristische Absicht, erforderlich. Es wird vorausgesetzt, dass die – zumindest geplante – Begehung der Straftaten nach der Vorstellung der Täter eine bestimmte politisch motivierte Zielsetzung verfolgt (so muss durch die Tatbegehung z. B. die Beseitigung der politischen Grundstrukturen eines Staates angestrebt werden).

Diese neuen Qualifikationsanforderungen wurden dabei **auch auf den früheren § 129a Abs. 1 Nr. 3 StGB erstreckt**, der in § 129a Abs. 2 Nr. 2 StGB aufgegangen ist.

Die Interessenschwerpunkte bei der Evaluierung dieser Norm lagen für das Projekt AGNES bei den Fragen, ob

- die Ermittlungspraxis durch den erweiterten Straftatenkatalog erleichtert wurde und
- sich Nachweisprobleme hinsichtlich der subjektiven Tatbestandselemente ergeben haben.

Diese Besonderheit der Kombination eines weit gefassten objektiven Tatbestandes mit hohen gesetzlichen Anforderungen an den subjektiven Tatbestand ist nur beim Absatz 2

[48] Gesetz vom 22.12.2003, BGBl. 2003 I S. 2836.
[49] Aufgeführt sind z.B. schwere Körperverletzung, Computersabotage, bestimmte Verstöße gegen das WaffG und das KWKG.

des § 129a StGB gegeben, nicht aber bei Absatz 1. Dieser wurde durch die Novellierung nur insofern geändert, als bestimmte Straftaten des ursprünglichen Kataloges in den Absatz 2 überführt wurden. Daher beschränkt sich das Projekt auf eine Evaluierung des neuen § 129a Absatzes 2 StGB.

Für den Bericht wurden 25 Fragebögen sowie zwei Expertengespräche zu Verfahren wegen des Verdachts einer Straftat nach § 129a Abs. 2 StGB ausgewertet. Im Folgenden werden die zentralen Erkenntnisse aus dieser Erhebung dargestellt.

2.1. Beurteilung des Anfangsverdachts

Bei der Einleitung von Verfahren nach § 129a Abs. 2 StGB ergaben sich ausweislich der Fragebögen und der geführten Expertengespräche in der polizeilichen Praxis keine Probleme.[50] Die im Gesetzgebungsverfahren geäußerte Befürchtung, die terroristische Absicht lasse sich nicht mit den nötigen tatsächlichen Anhaltspunkten belegen,[51] hat sich nicht verwirklicht.

Häufig wird jedoch in den Einleitungsverfügungen nicht zwischen Taten nach Absatz 1 und solchen nach Absatz 2 des § 129a StGB differenziert.

2.2. Tatbeteiligung sowie Katalogtaten

Die Erhebung umfasst 25 Ermittlungsverfahren wegen Gründung bzw. Beteiligung in einer terroristischen Vereinigung nach § 129a Abs. 2 StGB.
In nur einem der 25 Verfahren verblieb die beabsichtigte Gründung der Organisation im Stadium der straflosen Vorbereitungshandlung. Hier hatte der Tatverdächtige im Internet nach Mittätern für mögliche Selbstmordanschläge gesucht, der Anfangsverdacht strafbaren Verhaltens konnte aber nicht erhärtet werden.

Bei der Auswertung der erhobenen Daten zeigt sich, dass die Tatmodalitäten der verschiedenen Gruppierungen, soweit sie – wie üblich – in politische und religiöse Gruppen unterteilt werden, nicht miteinander vergleichbar sind.

[50] Die später unter 2.5. angesprochenen Probleme bei Ermittlungsverfahren in Bezug auf die Schädigungseignung der Tat haben auf die Einleitung der evaluierten Verfahren keine Auswirkungen gehabt, da diese Verfahren zum Zeitpunkt des Ergehens der unter 2.5. erwähnten Beschlüsse des BGH bereits längere Zeit betrieben wurden. Die erwähnten Probleme könnten allerdings dazu führen, dass in Zukunft die Annahme eines Anfangsverdachtes einer Straftat nach § 129a Abs. 2 StGB restriktiver gehandhabt wird.

Daher wird hier bei jeder Frage eine Differenzierung nach drei Gruppen von Organisationen vorgenommen, auf die sich die im Projekt erfassten Verfahren bezogen:

- politisch rechts motivierte,
- politisch links motivierte und
- islamistisch motivierte Vereinigungen.

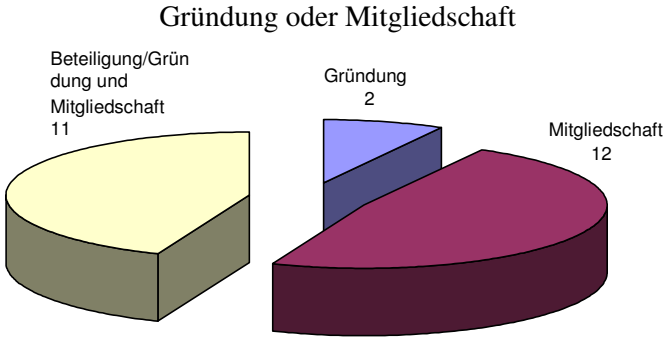
Die hier betrachteten Vereinigungen waren in 21 von 24 Fällen **politisch links motiviert**. Politisch rechts motiviert war eine Vereinigung und islamistisch motiviert waren zwei Vereinigungen.

Der Schwerpunkt der verübten terroristischen Delikte liegt nach dem „Jahreslagebild politisch motivierte Kriminalität 2006“[52] bei politisch motivierter Ausländerkriminalität (Islamismus). Diese unterfällt aber in der Regel §§ 129a Abs. 1, 129b StGB, da die Gruppierungen gerade darauf abzielen, Menschenleben zu gefährden.
Politisch rechts motivierte Vereinigungen begehen dem gegenüber ausweislich des Berichts hauptsächlich Propagandadelikte.
Da sich die Erhebung und Auswertung im Projekt AGNES auf Verfahren beschränkte, bei denen es um Taten nach § 129a Abs. 2 StGB ging, bezieht sich die nachfolgende Darstellung auf die politisch links motivierten Vereinigungen sowie auf einen Tatkomplex aus dem politisch rechten Spektrum. Die beiden Sachverhalte islamistisch motivierter Ausländerkriminalität wurden in die Untersuchung mit aufgenommen, da die Ermittlungsverfahren in diesen Fällen ausweislich der Zulieferung der ermittelnden Polizeibehörde wegen § 129a Abs. 2 StGB geführt wurden.

Innerhalb der jeweiligen Kategorien war die Modalität der **Tatbegehung** bei den analysierten Verfahren nach § 129a Abs. 2 StGB **jeweils vergleichbar**:
Bei den **politisch links** motivierten Vereinigungen erklärte jeweils ein Selbstbezichtigungsschreiben die Ziele der Gruppierung sowie deren Motivation. Die Gruppierung wurde den Ermittlungsbehörden somit spätestens durch dieses Bekennerschreiben bekannt, nicht zur Kenntnis gelangten jedoch die genauen Mitglieder.
Die von der Erhebung erfasste **politisch rechts** motivierte Vereinigung hinterließ kein Selbstbezichtigungsschreiben, weshalb das Vorliegen einer terroristischen Vereinigung

[51] Vgl. beispielsweise Protokoll der 21. Sitzung des Rechtsausschusses vom 4. Juni 2003, S. 6 und Bundestagsprotokoll 15/67, S. 5821 sowie S. 5836.
[52] Herausgegeben vom BKA, Abteilung Polizeilicher Staatsschutz.

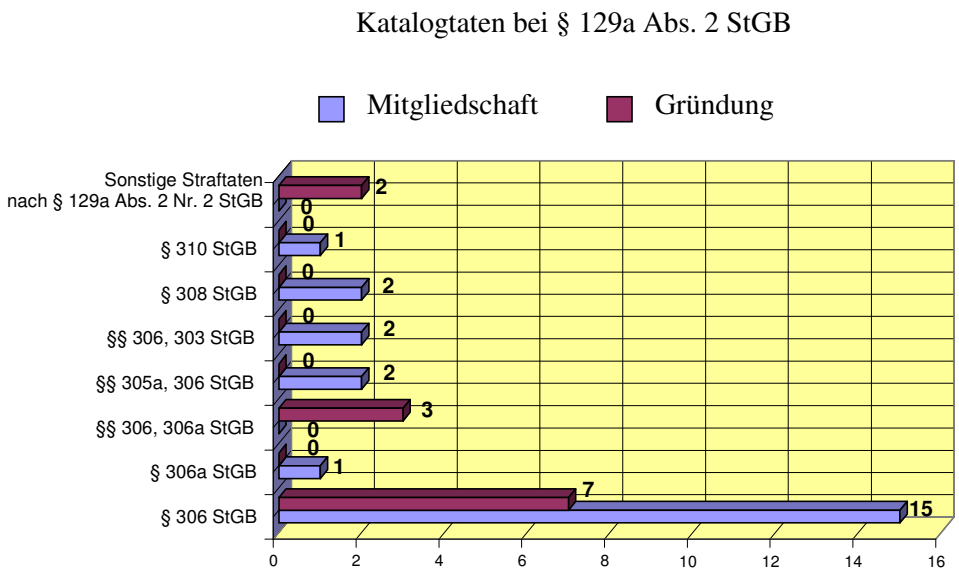
zunächst nicht erkennbar war. Die Ermittlungen wurden daher wegen bandenmäßiger Begehung vergleichbarer Straftaten geführt.



In 13 der 25 untersuchten Fälle wurde wegen Gründung, in 23 Fällen wegen mitgliedschaftlicher Beteiligung an einer terroristischen Vereinigung ermittelt.
Der Vorwurf, sowohl an der Gründung als auch als Mitglied in der Vereinigung beteiligt zu sein, wurde elf Mal erhoben. Allein wegen Gründung einer terroristischen Vereinigung wurden zwei Verfahren geführt, „nur“ wegen Mitgliedschaft zwölf Verfahren.
Die jeweilige Zuordnung „Verdacht der Gründung“ bzw. „Verdacht der Mitgliedschaft“ basiert bis auf ein Verfahren, in dem von den zwölf Angeklagten fünf wegen Gründung, alle anderen nur wegen Beteiligung als Mitglied verurteilt wurden, auf einer Einschätzung der Polizei im Ermittlungsverfahren.

Der **Tatbeitrag** der Tatverdächtigen bei **politisch links** motivierten Vereinigungen bestand in der Gründung bzw. Organisation einer terroristischen Vereinigung sowie in der Teilnahme an Brandanschlägen.

Bei den beiden **islamistisch** motivierten Vereinigungen bestand der Tatbeitrag in der Beteiligung an Schleusungen, Urkundenfälschungen und Vermögensdelikten oder sonstigen Finanzierung der Organisation. Die Beschuldigten der betrachteten **politisch rechts** motivierten Vereinigung beteiligten sich in unterschiedlicher Intensität an Brandstiftungen: eine Person als Rädelsführer (zum Teil nur mit der Tatplanung befasst), andere nur in untergeordneter Funktion (z.B. Botendienste).



Die Katalogtaten konzentrieren sich auf den Bereich der **Brandstiftungsdelikte.**

In den 13 Verfahren wegen Gründung einer terroristischen Vereinigung waren zehn Mal Taten nach § 306 StGB, davon drei Mal auch Taten nach § 306a StGB geplant. In zwei Fällen ging es um gemeingefährliche Straftaten in bestimmten Fällen, einmal um eine Tat nach § 308 StGB.

Hinsichtlich der 23 Verfahren wegen Beteiligung an einer terroristischen Vereinigung waren 17 Mal Straftaten nach § 306 StGB geplant, davon zwei Mal darüber hinaus auch Taten nach § 305a StGB. Zwei Mal ging es um Taten nach § 308 StGB und je ein Mal um solche nach § 306a StGB bzw. § 310 StGB.

2.3. Beschuldigte von Ermittlungsverfahren

Im Folgenden wird nicht zwischen Mitgliedern und Gründern der jeweiligen Vereinigung differenziert, da die Gründer einer Vereinigung in der Regel auch Mitglied in derselben sind. Bis auf zwei Verfahren, bei denen ausschließlich die Gründung einer terroristischen Vereinigung im Ermittlungsverfahren verfolgt wurde, ist dies in allen Verfahren berücksichtigt worden. Eine gleichzeitige Mitgliedschaft in der Vereinigung konnte vernachlässigt werden.
Sämtliche untersuchten Verfahren gegen **politisch links** motivierte Vereinigungen richteten sich (zunächst) gegen Unbekannt. Wurde ein Selbstbezichtigungsschreiben aufgefunden, konnten unmittelbar Rückschlüsse auf das Bestehen einer terroristischen

Vereinigung gezogen werden. Bekannte sich eine Gruppierung erst nachträglich zu einem Anschlag, konnten ab dann bzw. aufgrund vergleichbarer Tatmodalitäten Rückschlüsse auf das Vorliegen einer terroristischen Vereinigung gezogen werden.

Die Angaben zur Anzahl der Mitglieder der Vereinigung waren daher zunächst schwankend und reichten bis zu sechs Mitgliedern zu Beginn der Ermittlungen. 23 der 25 betrachteten Ermittlungsverfahren sind noch nicht abgeschlossen, so dass die genaue Anzahl der Mitglieder der jeweiligen Vereinigung noch nicht endgültig ermittelt werden konnte.

Bei der betrachteten **politisch rechts** motivierten Vereinigung waren zwar die Tatbeteiligten bekannt (zwölf Mitglieder), es wurde jedoch zunächst ausschließlich wegen Brandstiftungsdelikten ermittelt. Erst nach einer Vernehmung der Tatverdächtigen wurden die Ermittlungen auf den Tatbestand der Gründung und Mitgliedschaft in einer terroristischen Vereinigung ausgeweitet.

2.4. Dauerhaftigkeit der Vereinigung

Das Erfordernis, dass die Organisation auf längere Dauer angelegt sein muss, war bei allen betrachteten Verfahren eindeutig erfüllt. Die Vereinigungen waren aber auf recht unterschiedliche **Dauer** angelegt. Die Zeitspanne reicht dabei von knapp zwei bis zu mehr als sechs Jahren. Die betrachteten Vereinigungen existierten zum Zeitpunkt der Ermittlungen alle bereits über einen Zeitraum von mindestens **eineinhalb Jahren**, so dass kein Zweifel daran bestand, dass das Kriterium der hinreichenden Dauer erfüllt war.

2.5. Eignung der Tat zu einer ernsthaften Schädigung

Die Katalogtaten müssen die **objektive Eignung** aufweisen, durch die Art ihrer Begehung oder ihre Auswirkungen einen erheblichen Schaden für einen Staat oder eine internationale Organisation hervorzurufen. Hierbei ist ausreichend, wenn die intendierte Durchführung oder die möglichen Folgen der Tat gefährlich für die Schutzgüter sein können. Ein konkreter Schadenseintritt oder auch nur dessen Wahrscheinlichkeit sind nicht erforderlich.[53] Folglich genügt die realistische Möglichkeit, dass der Schaden nach den Umständen der Tatbegehung eintreten kann. Ausreichend zur Bejahung der Eignung der

[53] BGH StB 43/07, S. 11 mit weiteren Nachweisen.

Tat zu einer erheblichen Schädigung der Schutzgüter ist nach BGH[54] die so genannte **Nadelstich-Taktik**. Danach reicht die Intention, durch eine Vielzahl von Einzeltaten eine der oben genannten Schädigungswirkungen zu erzielen.

Dass die Tat geeignet wäre, einen Staat oder eine internationale Organisation erheblich zu schädigen, wurde in den untersuchten Verfahren bei politisch links motivieren Vereinigungen in 2/3 der Verfahren belegt durch

- die Vielzahl der verübten (Brand-)Anschläge,
- die Art der Durchführung der Tat sowie
- den Inhalt des Selbstbezichtigungsschreibens,

was jeweils auf eine **fest organisierte Vereinigung** mit dem **Ziel, Straftaten gleicher Schwere und Art auch in Zukunft zu begehen**, hindeutete.

Der zentrale Ermittlungsansatz beim Verdacht der Bildung einer **politisch links** motivierten terroristischen Vereinigung war in den untersuchten Fällen jeweils das **Selbstbezichtigungsschreiben**. In diesem wurden in der Regel die Opfer genau beschrieben und die Gründe für den geplanten Umsturz des Systems dargelegt.

Die Selbstbezichtigungsschreiben, die von (links-)**autonomen Gruppen** stammten, stellten explizit darauf ab, dass Menschen nicht gefährdet werden sollen. Da die Tatmodalitäten den Angaben in den Schreiben entsprachen, scheidet eine Strafbarkeit nach § 129a Abs. 1 StGB, der als Katalogtaten ausschließlich Delikte aufführt, die Menschen gefährden, in Bezug auf die hier betrachteten autonomen Gruppen aus.

In drei der aufgefundenen Bekennerschreiben links motivierter Vereinigungen wurde jeweils angegeben, die Gruppierung plane einen gewaltsamen Umsturz in Deutschland bzw. die Beseitigung der verfassungsrechtlichen Grundstrukturen Deutschlands. Durch die verübten Taten sowie die Auswahl der Anschlagsziele versuchten die Tatverdächtigen, Verfassungsorganen ihren politischen Willen aufzuzwingen. Beispielsweise wurde in einem staatsanwaltschaftlichen Eröffnungsbeschlussantrag angenommen, dass aus der Zerstörung großer Anlagen international tätiger Unternehmen die Eignung folge, den Staat Deutschland zu schädigen.

[54] BGH StV 2006, 691.

In einem der zwei betrachteten Fälle **islamistisch motivierter** Vereinigungen sollten vermeintlich islamfeindliche, insbesondere US-amerikanische Personen und Einrichtungen bzw. mit den USA im Irakkrieg alliierte Personen und Einrichtungen angegriffen werden. Die andere in die Untersuchung einbezogene islamistisch motivierte Vereinigung wollte Geldmittel für die Organisation „Ansar al-Islam“[55] beschaffen sowie einen Sprengstoffanschlag vorbereiten.

Die erfasste **rechts motivierte** terroristische Vereinigung plante mittels einer Vielzahl von Brandanschlägen gegen von Ausländern geführte Gewerbebetriebe, zumindest einen Teil Deutschlands „ausländerfrei“ zu machen.

Es hat sich gezeigt, dass es für die Polizei und Staatsanwaltschaft in den betrachteten Fällen keine Schwierigkeiten gab, die Eignung einer Tat zur ernsthaften Schädigung der in § 129a Abs. 2 StGB genannten Schutzgüter zu bejahen. Allerdings muss, wie bereits erwähnt, beachtet werden, dass die Verfahren zum Zeitpunkt der Datenerhebung noch nicht abgeschlossen waren.

Zwei der betrachteten politisch links motivierten Verfahren haben inzwischen aufgrund von Erkenntnissen, die zu Beginn der jeweiligen Ermittlungsverfahren noch nicht vorlagen, eine rechtlich andere Beurteilung erfahren. So schätzte der BGH Ende 2007 in zwei Fällen die Eignung einer terroristischen Vereinigung, einen Staat ernsthaft zu schädigen, anders ein als die Polizei und der zuständige Generalbundesanwalt bzw. der Ermittlungsrichter beim BGH:

- In der einen Entscheidung des BGH[56] über Haftbeschwerden mehrerer Beschuldigter in einem Ermittlungsverfahren wegen des Verdachts der Mitgliedschaft in der politisch links motivierten terroristischen Vereinigung „militante gruppe“ (mg) wurde die objektive Eignung, die Bundesrepublik Deutschland mittels Brandanschlägen gegen Gebäude und Fahrzeuge in der im Verfahren relevanten Form erheblich zu schädigen, verneint. Nach Ansicht des BGH muss die Möglichkeit der erheblichen Schädigung jeweils unter Berücksichtigung aller Umstände des Einzelfalls geprüft werden. Eine nennenswerte Beeinträchtigung der Tätigkeit der betroffenen staatlichen und privaten Stellen sei in dem Fall weder eingetreten noch

[55] Ansar al-Islam ist eine Organisation, die für einen islamistischen Nationalstaat im kurdischen Teil des Irak kämpft.
[56] Vgl. Beschluss vom 28.11.2007, StB 43/07.

zu erwarten gewesen; mittelbare Folgen aufgrund eigenständigen Handelns Dritter – also insbesondere potentielle Mobilisierungseffekte bei Gleichgesinnten – seien irrelevant.

Aus der BGH-Entscheidung die Schlussfolgerung zu ziehen, dass bei ausschließlicher Gewalt gegen Sachen das Vorliegen einer terroristischen Vereinigung generell ausscheide, wäre unzutreffend. Der gleiche Senat des BGH hat in seinem Beschluss ausdrücklich auf seine Entscheidung im Freikorps-Verfahren[57] verwiesen, dem ausschließlich Brandanschläge gegen Sachen zugrunde lagen, und in dem er eine Strafbarkeit nach § 129a Abs. 2 StGB bejaht hatte. Der Unterschied liege in der Beeinträchtigung des Sicherheitsgefühls der ausländischen Bewohner, was zu deren Fortzug und einer Schwächung des Vertrauens in die Wirkungskraft elementarer Verfassungsgrundsätze hätte führen können.

Konsequenz der Entscheidung für das so genannte mg-Verfahren war, dass „nur" noch der Verdacht einer Strafbarkeit wegen Mitgliedschaft in einer kriminellen Vereinigung nach § 129 StGB gegeben war, die Strafverfolgungszuständigkeit blieb gemäß § 74a Abs. 1 Nr. 4 GVG aber aufgrund der besonderen Bedeutung des Falles weiterhin beim GBA.

- Die zweite Entscheidung des BGH aus dem Jahr 2007 zu § 129a Abs. 2 StGB erging anlässlich der Beschwerde eines Beschuldigten gegen eine Durchsuchungsanordnung. In dieser Entscheidung nimmt der BGH[58] Stellung zu der Frage, ob zwölf Anschläge mit einem Gesamtschaden von 2,6 Millionen Euro eine erhebliche Schädigung des Staates darstellen, und verneint dies. Weder die Art der Begehung, konkret also ihre Häufigkeit und Intensität, noch die Auswirkungen der Anschläge seien geeignet gewesen, einen erheblichen Schaden für die Bundesrepublik Deutschland zu bewirken. Eine Gefährdung von Menschen sei von der Gruppierung ausgeschlossen worden und eine nennenswerte Behinderung der Tätigkeit des Staates oder staatlicher Organe sei nicht eingetreten. Die Straftaten, zwölf Brandanschläge auf Kraftfahrzeuge mehrerer Wirtschaftsunternehmen und deren Repräsentanten sowie eines Staatssekretärs und Sachbeschädigungen an Gebäuden, unter anderem auf ein im Bau befindliches Gästehaus des Auswärtigen Amtes, seien solche der mittleren Kriminalität.

[57] Vgl. BGH NJW 2006, 1603.
[58] Vgl. BGH NStZ 2008, 146 ff.

Fernziele der Gruppierung seien sowohl „Propaganda“ als auch die Mobilisierung von Gesinnungsgenossen für Proteste anlässlich des Weltwirtschaftsgipfels gewesen. Mögliche mittelbare Folgen – Dritte folgen dem Aufruf und begehen Straftaten – müssten bei der Betrachtung der Schädigungseignung der terroristischen Vereinigung unberücksichtigt bleiben. Die Mobilisierung sei dann zwar kausal, nicht aber der Gruppierung zurechenbar, da sie auf eigenständigem Handeln Dritter beruhe.

Bei konkreter Betrachtung sei von der Propaganda der Gruppierung zudem allenfalls ein schwacher Anreiz zur Begehung vergleichbarer Taten ausgegangen.

Die Darstellung, die Gruppierung arbeite konspirativ, sei kein Argument für die Bejahung einer Eignung zur erheblichen Schädigung, da alle Vereinigungen im Sinn von §§ 129 und 129a StGB typischerweise konspirativ vorgingen.

Als Konsequenz aus dieser Rechtsprechung ist die Eignung zu einer erheblichen Schädigung auf jeden Fall dann anzunehmen, wenn mit den (geplanten) Taten erreicht werden kann, dass der Staat oder eine internationale Organisation vollständig oder zumindest partiell unfähig wird, die ihm/ihr obliegenden Aufgaben ordnungsgemäß zu erfüllen – beispielsweise durch nicht nur rein lokal wirkende Angriffe auf die Energieversorgung. Folgen ohne spürbare Auswirkungen, wie etwa der Verlust einzelner Kraftfahrzeuge, genügen dagegen nicht.
Dabei ist zu beachten, dass an die Beurteilung der Schädigungseignung im Lauf des Ermittlungsverfahrens unterschiedliche Anforderungen gestellt werden: Je weiter das Verfahren fortgeschritten ist, umso konkreter müssen die Erkenntnisse zur Schädigungseignung sein.

Im Gesetzgebungsverfahren zu § 129a Abs. 2 StGB im Jahr 2003 wurde von Seiten der geladenen Sachverständigen im Rahmen einer Anhörung vor dem Rechtsausschuss des Bundestages gemutmaßt, dass durch die Neuregelung vor allem bei Ermittlungsverfahren gegen militante und autonome Gruppierungen nur noch eine Strafverfolgung nach § 129 StGB in Betracht komme.[59] Auch wenn die beiden vorstehend erwähnten Entscheidungen des BGH diese Einschätzung zu bestätigen scheinen, darf nicht verkannt werden, dass in Einzelfällen auch solche militanten und autonomen Gruppierungen denkbar sind, die die engen Voraussetzungen des § 129a Abs. 2 StGB erfüllen.

[59] Vgl. Zusammenfassung in BGH StB 43/07, S. 15 f.

2.6. Ziel der Vereinigung, Taten mit einer gewissen Bestimmung zu begehen

Ziel der Vereinigung muss nach § 129a Abs. 2 StGB die Herbeiführung einer der folgenden Wirkungen sein:

- Erhebliche Einschüchterung der Bevölkerung; ausreichend ist hier, dass die Tat gegen nennenswerte Teile der Gesamtbevölkerung gerichtet ist,[60]
- Nötigung einer Behörde oder internationalen Organisation mit Gewalt oder durch Drohung mit Gewalt,
- Beseitigung oder erhebliche Beeinträchtigung der politischen, verfassungsrechtlichen, wirtschaftlichen oder sozialen Grundstrukturen eines Staates oder einer internationalen Organisation.

Für die Bejahung dieses subjektiven Elementes ist z.B. das Ziel ausreichend, im Rahmen eines revolutionären Kampfes eine kommunistische Staats- und Gesellschaftsordnung für die Bundesrepublik Deutschland anzustreben.

Die im Projekt betrachteten Selbstbezichtigungsschreiben der links motivierten Vereinigungen waren einander sehr ähnlich und belegten alle das Ziel der agierenden Gruppierungen, den Umsturz des aktuellen politischen Systems herbeizuführen. Dies wurde in allen Verfahren seitens der Polizei als ausreichend für die Bejahung eines Anfangsverdachtes einer Strafbarkeit nach § 129a Abs. 2 StGB erachtet.

2.7. Schlussfolgerungen

§ 129a Abs. 2 StGB ist in seiner derzeitigen Fassung zwar als Norm für die Polizei handhabbar, doch hat die jüngste Rechtsprechung des BGH bewirkt, dass Ermittlungsverfahren gegen militante und autonome Gruppen des derzeit typischen Zuschnitts nur noch in besonders gelagerten Fällen unter § 129a Abs. 2 StGB subsumiert werden können. Der Anwendungsbereich des früheren § 129a Abs. 1 Nr. 3 StGB hat sich damit nach Angaben der Polizeipraxis signifikant reduziert.

Angesichts der von der Rechtsprechung geforderten restriktiven Handhabung des objektiven Tatbestandsmerkmals „erhebliche Schädigung“ ist dieses Merkmal auf jeden Fall dann zu bejahen, wenn die Anlasstaten geeignet sind, die gänzliche oder teilweise Unfähigkeit der Ausübung staatlicher Funktionen oder der Funktionen einer der genannten

Organisationen herbeizuführen und damit den Staat als solchen oder die Organisation als solche zu schädigen. Hierbei ist zu beachten, dass sich die Anforderungen an die Beurteilung, dass eine Tat zur ernsthaften Schädigung der erfassten Schutzgüter geeignet ist, im Lauf des Ermittlungsverfahrens verändern. Je fortgeschrittener das Verfahren ist, desto konkreter müssen die tatsächlichen Anhaltspunkte für das Vorliegen einer Schädigungseignung sein.

Die bislang ergangenen gerichtlichen Entscheidungen zur Schädigungseignung bei § 129a Abs. 2 StGB zeigen, dass eine Einzelfallbetrachtung stets erforderlich ist. Brandstiftungen, die Gewerbestätten ausländischer Gewerbetreibender in Deutschland betrafen und die mit der Intention verübt wurden, eine ausländerfreie Region zu schaffen, erfüllten nach Ansicht der Rechtsprechung die tatbestandlichen Anforderungen des § 129a Abs. 2 StGB, wenn sie geeignet sind, die betroffene Bevölkerungsgruppe zum Wegzug zu motivieren. Brandstiftungen, die Kfz und Gebäude betrafen, ohne dass jedoch von den Tatverdächtigen mit der Tatbegehung ein derartiges Ziel verfolgt wurde (dessen Erreichen das Vertrauen in die Wirkungskraft elementarer Verfassungsgrundsätze schwächen würde), unterfielen jedoch dem Tatbestand des § 129a Abs. 2 StGB trotz hohen entstandenen Sachschadens nach Ansicht der Rechtsprechung nicht ohne Weiteres. Es wurde im Ergebnis zwischen dem unmittelbaren Nahziel der Tat (Wegfall einiger Kraftfahrzeuge, der an sich nicht zu den genannten Schäden führt) und einem Fernziel, dessen Eintritt erst über eine ganze Kette weiterer Umstände erfolgen könnte (Appellwirkung; Motivation zu weiteren Straftaten; „Schneeballeffekt“; erst dann ernsthafte Schädigung des Staates) unterschieden. Entscheidender Unterschied zwischen den „Freikorps“- und den „mg“-Fällen ist nämlich, dass in den „Freikorps“-Fällen Dritte, die nicht den Zielen der Vereinigung anhängen, unmittelbar durch die Taten den nachhaltigen Eindruck erlangen sollten, die Rechtsordnung werde regional nicht mehr gesichert, während in den „mg“-Fällen erst eigene Anhänger oder Sympathisanten zu weiteren strafbaren Handlungen motiviert werden sollten, wobei erst durch solche Taten eine ernsthafte Gefährdung des Staates an sich bewirkt werden könnte.

Insbesondere bei politisch motivierter Gewaltkriminalität gegen Sachen, bei der eine Gefährdung von Menschenleben ausgeschlossen wurde, hängt von den näheren Tatumständen ab, ob der Tatbestand des § 129a Abs. 2 StGB gegeben und nachzuweisen ist.

[60] Vgl. BGH NJW 2006, 1603.

Sofern darüber hinaus mangels eines Anhaltspunktes für das Vorliegen einer Vereinigung auch eine Strafbarkeit nach § 129 StGB abgelehnt wird[61], kann ein Ermittlungsverfahren nur wegen der jeweiligen Katalogtaten geführt werden. Da diese für eine Strafbarkeit nach § 129a Abs. 2 StGB jedoch noch nicht verübt worden sein müssen, kann sich die dann in Betracht kommende Tat noch im Stadium der straflosen Vorbereitung oder eines straflosen Versuchs befinden.

Die – soweit ersichtlich – bislang einzige Verurteilung nach § 129a Abs. 2 StGB erfolgte in Bezug auf eine politisch rechts motivierte Vereinigung. Bisher in Deutschland aktiv gewordene islamistisch motivierte Vereinigungen haben bei ihren Taten jeweils eine Gefährdung von Menschenleben in Kauf genommen, weshalb die Verantwortlichen in Anwendung des § 129a Abs. 1 StGB verurteilt wurden.

2.8. Prüfungsschema für § 129a Abs. 2 StGB

Nachfolgendes Prüfungsschema richtet sich an Sachbearbeiter, welche die Einleitung eines Ermittlungsverfahren aufgrund eines Anfangsverdachts nach § 129a Abs. 2 StGB in Betracht ziehen.

1. Begriff der Vereinigung

- Eine Vereinigung ist ein auf längere Dauer angelegter organisierter Zusammenschluss von mindestens drei Personen, die bei Unterordnung des Willens des Einzelnen unter den Willen der Gesamtheit gemeinsame Zwecke verfolgen und unter sich derart in Beziehung stehen, dass sie sich untereinander als einheitlicher Verband fühlen.

2. Vorliegen einer der abschließend aufgezählten Straftaten

- Der Zweck der Vereinigung muss auf die Begehung einer der im Katalog genannten Tat gerichtet sein.

Eine einmalige Begehung einer Katalogtat ist nicht ausreichend.

3. Schädigungseignung der Taten

- Eignung der Tat zu einer ernsthaften, erheblichen Schädigung eines Staates oder einer internationalen Organisation
  - durch die Art der Begehung oder
  - ihre Auswirkungen.

[61] Vgl. Beschluss des BGH NStZ 2008, 146 ff.

- Der Durchführung bzw. den Folgen der Straftat muss eine konkrete Gefährlichkeit anhaften. Ein konkreter Schadenseintritt ist nicht erforderlich.
- Erheblich ist die Schädigung, wenn sie deutlich spürbare Auswirkungen zeigt, beispielsweise die vollständige oder teilweise, ggf. auch regional begrenzte Unfähigkeit bzw. deutlich geminderte Fähigkeit des Staates oder der internationalen Organisation, die obliegenden Aufgaben wie Bereitstellung von Infrastruktur, Sozialwesen, Wahrung der öffentlichen Sicherheit ordnungsgemäß zu erfüllen. Es ist nicht erforderlich, dass das Staatswesen als Ganzes beeinträchtigt ist, wenn eine Eignung zur Schädigung der Fähigkeit zur Wahrnehmung staatlicher Funktionen, auch regional und auf einzelne Aufgaben beschränkt, konkret nachgewiesen werden kann.

Die Eignung einer Tat kann sich auch aus dem Zusammenhang mit weiteren geplanten Straftaten ergeben.

4. Bestimmung der Taten

Die von der Vereinigung geplante Katalogtat muss dazu bestimmt sein (subjektives Element),

- **Variante 1:**…die Bevölkerung auf schwerwiegende Weise einzuschüchtern.

Wenn das Sicherheitsgefühl eines zumindest wesentlichen, nennenswerten Teils derart betroffen ist, dass das Vertrauen in die öffentliche Rechtssicherheit und das befriedete Zusammenleben der Bürger massiv beschädigt oder gar erschüttert ist, so dass die Wahrnehmung elementarer, für das Zusammenleben unabdingbarer Grundfreiheiten des Einzelnen gefährdet wird. Die Einschüchterung ist vergleichbar mit einer Störung des öffentlichen Friedens im Sinn von § 126 StGB.

- **Variante 2:**…eine Behörde oder internationale Organisation mit Gewalt oder durch Drohung mit Gewalt zu nötigen.

Es reichen einzelne Mitarbeiter aus, die mit der Nötigung beabsichtigten Folgen müssen eine vergleichbare Qualität wie die erste Variante aufweisen.

- **Variante 3:**…die politischen, verfassungsrechtlichen, wirtschaftlichen oder sozialen Grundstrukturen eines Staates oder einer internationalen Organisation zu beseitigen oder erheblich zu beeinträchtigen.

Ein konkreter Schadenseintritt ist nicht erforderlich. Erheblich ist die Schädigung, wenn sie deutlich spürbare Auswirkungen zeigt, beispielsweise bei Angriffen auf die Integrität des Staates oder einer internationalen Organisation, durch den die Sicherung der das Gemeinwesen konstituierenden Strukturen und die Gewährleistung grundlegender rechtsstaatlicher Prinzipien wesentlich gefährdet würden wie bei Anschläge auf zentrale

Infrastruktur- oder Versorgungseinrichtungen, auf Regierungsstellen, Amtsgebäude, Informatiksysteme oder bedeutende Finanzzentren eines Staates.

Die Bestimmung einer Tat kann sich auch aus dem Zusammenhang mit weiteren geplanten Straftaten ergeben.

3. Themenkomplex: Ermittlungspraxis im Zusammenhang mit der Nutzung moderner Kommunikationsmittel

Dieser Themenkomplex beschäftigt sich mit den Auswirkungen der informationstechnischen Entwicklung auf die Verfolgbarkeit von Kriminalität und damit einhergehend mit der Problematik des Schritthaltens der Polizei mit dem „Gegenüber“.

Daneben gilt es, neue modi operandi, das heißt auf der Entwicklung moderner Kommunikationsmittel beruhende neue Kriminalitätsformen, frühzeitig zu erkennen und ihnen zu begegnen. Die besondere Relevanz dieses Themenkomplexes für die Polizeipraxis ergibt sich aus der Tatsache, dass die aktuelle Kriminalitätsentwicklung zwar erkannt und die Notwendigkeit einer polizeilichen Reaktion auf neues Täterverhalten gesehen wird, bei der Handhabung geltender Normen jedoch große Unsicherheit auch seitens der Justiz besteht. Gefestigte Rechtsprechung, an der sich die Anwendung bestimmter Normen orientieren könnte, existiert bisher nicht.

Dies hat sich vor allem bei der beachtlichen öffentlichen Diskussion zur so genannten Online-Durchsuchung, aber auch bei anderen polizeilichen Ermittlungsmaßnahmen im Zusammenhang mit modernen Kommunikationsmitteln, etwa der verdeckten Teilnahme an geschlossenen Chats und dem verdeckten Zugriff auf zwischengespeicherte Daten, gezeigt.

3.1. Online-Durchsuchung

Der Begriff der "Online-Durchsuchung" ist nicht legaldefiniert, sondern wurde etwa in dem Aufsatz von Hofmann in NStZ 2005, S 121 ff. aufgegriffen und seitens BKA mit folgender Arbeitsdefinition für die taktisch-technische Entwicklung entsprechender Einsatzszenarien belegt: Demnach ist die Online-Durchsuchung nach hiesigem Verständnis die verdeckte Suche unter Einsatz elektronischer Mittel nach verfahrensrelevanten Inhalten auf informationstechnischen Systemen, die sich nicht im direkten physikalischen Zugriff der Polizeibehörden befinden, aber über Kommunikationsnetze erreichbar sind. Gegenstand der Suche sind ausschließlich Daten, die nicht im Wege eines aktuellen Telekommunikationsvorgangs übermittelt werden.

Die Maßnahme kann subsumiert werden unter die in § 20k des BKAG-E (Stand: 25.08.08) vorgesehene Regelung, wonach unter den dort genannten engen Voraussetzungen ohne Wissen des Betroffenen mit technischen Mitteln in vom Betroffenen genutzte

informationstechnische Systeme eingegriffen werden kann und aus ihnen Daten erhoben werden können. Dabei wird zwar der Begriff der "Online-Durchsuchung" nicht explizit benannt, gesetzestechnisch ist der Tatbestand jedoch notwendigerweise abstrahiert.

Eine Online-Durchsuchung in diesem Sinne ist weder der offene Zugriff auf Daten noch die so genannte Quellen-TKÜ, die sich ausschließlich auf das Erlangen laufender Telekommunikationsinhaltsdaten richtet (so auch die amtliche Begründung zum Entwurf des BKAG, zu § 20k BKAG-E).

Wird die Suche und Erhebung kontinuierlich und längerfristig durchgeführt, um Veränderungen auf dem System erkennen und ermitteln zu können, wird die Maßnahme im polizeilichen Sprachgebrauch als **Online-Überwachung** bezeichnet. Diese ist deutlich eingriffsintensiver als ein einmaliger Zugriff im Rahmen einer punktuellen Online-Durchsuchung.

Dass die derzeitige Rechtslage **keine** Online-Durchsuchung zulässt, ist seit der diesbezüglichen Entscheidung des BGH vom 31.01.2007[62] geklärt. Insofern sei an dieser Stelle vorab erwähnt, dass das Thema "Online-Durchsuchung" ab dem Zeitpunkt dieser BGH-Entscheidung nicht streng unter den Projekttitel "Auswirkungen gesetzlicher Neuregelungen" subsumiert werden konnte, da eine solche (neue) gesetzliche Regelung der Online-Durchsuchung während des Erhebungszeitraums gerade nicht bestand. Folglich konnten die am Projekt beteiligten polizeilichen Dienststellen auch keine aktuellen "Anregungen" oder "Beantragungen" oder gar "Durchführungen" von Online-Durchsuchungen aus dem Erfassungszeitraum ab 31.01.07 zuliefern, diese steuerten jedoch über Erkenntnisse zum erkannten gesetzlichen Neuregelungsbedarf hinaus zusätzliche Erwägungen bei, die gleichwohl in diesen Projektbericht eingeflossen sind.

Die Entscheidung des BGH hat mediale und auch polizeiinterne Aufmerksamkeit erfahren, Es wurde deutlich, dass die Online-Durchsuchung nicht durch § 102 StPO (Durchsuchung bei Verdächtigen/Beschuldigten) gedeckt ist. Denn nach Auffassung des BGH wäre diese in § 102 StPO als offen durchzuführende Ermittlungsmaßnahme ausgestaltet, was sich in Anwesenheitsrechten gemäß § 106 Abs. 1 Satz 1 StPO sowie der Hinzuziehung von Zeugen nach §§ 105 Abs. 2, 106 Abs. 1 Satz 2 StPO zeige. Diese Normen stellten keine bloßen Ordnungsvorschriften, sondern zwingendes Recht dar und stünden nicht zur Disposition durch die Strafverfolgungsbehörden. Eine verdeckte Durchsuchung sei auch

keine den Betroffenen weniger belastende Maßnahme als eine offene Durchsuchung. Zudem zeige ein Vergleich mit den gesetzlichen Vorgaben für eine Telekommunikations- und Wohnraumüberwachung, dass an verdeckte Maßnahmen deutlich höhere formelle und materielle Anforderungen gestellt würden, als dies bei der Durchsuchung der Fall sei.
Auch andere Befugnisnormen wie §§ 100a, 100c oder 100f der StPO gestatteten keine verdeckte Online-Durchsuchung. Die Generalklausel des § 161 StPO erlaube nur geringfügige Grundrechtseingriffe, eine Online-Durchsuchung stelle dagegen einen erheblichen Eingriff in Grundrechte des Betroffenen dar.
Und schließlich könne eine Online-Durchsuchung auch nicht auf eine Kombination von verschiedenen Eingriffsbefugnissen wie §§ 102, 100a, 100c StPO gestützt werden, da damit dem Gesetzesvorbehalt für Eingriffe in Grundrechte und dem Grundsatz der Normenklarheit nicht genügt werde.

Inwieweit verfassungsrechtliche Vorgaben der Schaffung einer entsprechenden Befugnisnorm Schranken setzen, ergibt sich aus der Entscheidung des BVerfG zu § 5 des Verfassungsschutzgesetzes von Nordrhein-Westfalen.[63]

Für diesen Bericht wurden sieben Fragebögen sowie zehn Expertengespräche ausgewertet, die sich mit der Frage befassten, ob, und wenn ja, in welchem Umfang polizeilicher Bedarf an der Schaffung einer Rechtsnorm zur Online-Durchsuchung besteht. Im Folgenden werden die hieraus gewonnenen zentralen Erkenntnisse präsentiert.

3.1.1. Bedarf an der Normierung einer Ermächtigungsgrundlage zur Durchführung einer repressiven Online-Durchsuchung

Konkreter Bedarf für eine Online-Durchsuchung wird ausweislich der Fragebögen für die folgenden Fallkonstellationen gesehen:

- Sicherung bereits abgeschlossener, verschlüsselt **gespeicherter** Kommunikation (auch teilweise als "geronnene" Kommunikation bezeichnet), z.B. Daten aus zurückliegendem E-Mail-Verkehr, ICQ-Gesprächsverlauf, z.T. mittels Steganografie und PGP;
- Sicherung von Dokumenten vor der Ver- bzw. nach der Entschlüsselung. Hierzu gehören auch:

[62] Vgl. BGH MMR 2007, 237 ff.
[63] Vgl. BVerfG NJW 2008, 822 ff. Vgl. hierzu unter 3.1.6.

  - die Nutzung von privaten Postfächern mit geschlossenem Nutzerkreis ohne Datenaustausch und damit – mangels Kommunikation – ohne Möglichkeit einer TKÜ, sofern die Daten lokal auf einem Rechner gespeichert sind, und
  - Straftaten, bei denen tatrelevante Daten nicht im Netz, sondern lokal auf der Festplatte gespeichert sind, z.B. bei Attentatsvorbereitungen, wenn ein offenes Herangehen an den Rechner ausgeschlossen ist, da die Offenheit der Maßnahme weitere Ermittlungsansätze endgültig vereiteln würde.
- Sicherung unverschlüsselter Daten, wenn der PC gewohnheitsmäßig nach Benutzung verschlüsselt wird;
- Feststellen von Passwörtern und genutzten Programmen (insbesondere wichtig bei Verwendung von Steganografie und PGP) zur Entschlüsselung von Dateien.

Die Erforderlichkeit von Online-Durchsuchungen ergibt sich nach den Evaluationsergebnissen unter anderem daraus, dass Tatverdächtige oftmals Passwörter für ihren Rechner nicht preisgeben und folglich - jenseits taktischer Erwägungen - eine **offene Durchsuchung** (§§ 102 ff. StPO) mit anschließender Beschlagnahme (§§ 94, 98 StPO) und Datenauswertung bei einem passwortgeschützten Rechner von vornherein keinen Zugang zu den gespeicherten Daten ermöglicht. Außerdem besteht die Möglichkeit einen Rechner derart zu konfigurieren, dass bei Starten des Rechners durch einen fremden Nutzer bzw. in einer anderen als der üblichen Reihenfolge die Daten automatisch gelöscht werden und nach dem Löschen nicht wieder herstellbar sind. Auch in diesen Fällen wäre eine Durchsuchung nicht Erfolg versprechend.

Neben den vorstehend genannten Gründen wurde ein **Bedarf an einer Online-Durchsuchung** aufgrund folgender Aspekte artikuliert:

- Schwierigkeiten bereite das Sicherstellen von auf dem Computer bearbeiteten und anschließend auf externen Medien gespeicherten Dateien (z.B. USB-Stick), da diese Speichermedien bei einer konventionellen Durchsuchung aufgrund ihrer Größe häufig nicht gefunden werden könnten.
- In bestimmten Phänomenbereichen wie beispielsweise Spionage und Proliferation sowie in OK-relevanten Verfahren wegen gewerbsmäßiger Steuerhinterziehung, BtM- oder Waffenschmuggels und bei Zielfahndungsfällen sei die Gewinnung von Beweismitteln und weiteren Ermittlungsansätzen schwierig, da in diesen Fällen die

Tathandlungen durch ein äußerst konspiratives Vorgehen der Beschuldigten kennzeichnet seien.

- Vielfach sei es vor einer offenen Durchsuchung erforderlich, durch verdeckte Ermittlungen zu erforschen, wo der Beschuldigte tatrelevante Beweismittel – auf seinem PC oder anderswo – verberge bzw. wie er seinen PC für tatrelevante Kommunikation mit seinen Mittätern nutze, da offene Durchsuchungen ansonsten ergebnislos verliefen.

In Bezug auf die Terrorismusbekämpfung, ist nach Ansicht der befragten Dienststellen die Online-Durchsuchung aufgrund der Abschottung der Tatverdächtigen zur **Bekämpfung terroristischer und extremistischer Aktivitäten** zielführend, was sich auch bereits z.B. aus den Erfahrungen der EG Zeit im besonderen Maße ergeben hat. Beim islamistischen Terrorismus ist das Gefährdungspotenzial zwar nach Ansicht des Staatsschutzes größer als bei anderen Terrorismusformen. Sinnvoll ist dieses Ermittlungsinstrument aber in allen Bereichen des Terrorismus/Extremismus, in denen durch die Tatverdächtigen Textdateien z.B. in Form von Selbstbezichtigungsschreiben verfasst werden. Der linksextremistische Bereich ist extrem konspirativ. Hier agieren teilweise äußerst intelligente Tatverdächtige, die genaue Kenntnis von den Möglichkeiten und Grenzen polizeilichen Handelns bei TKÜ-Maßnahmen, klassischen Beschlagnahmen und E-Mail-Überwachungen haben, so dass solche Maßnahmen hier nicht weiterhelfen. Überdies gibt es nach Auskunft des Staatsschutzes Provider, die damit werben, dass sie keine E-Mail-Überwachung im Auftrag der Polizei durchführen. Ein Account bei einem solchen Provider ist nur über „Freundschaftswerbung“ in der Szene zu erlangen.

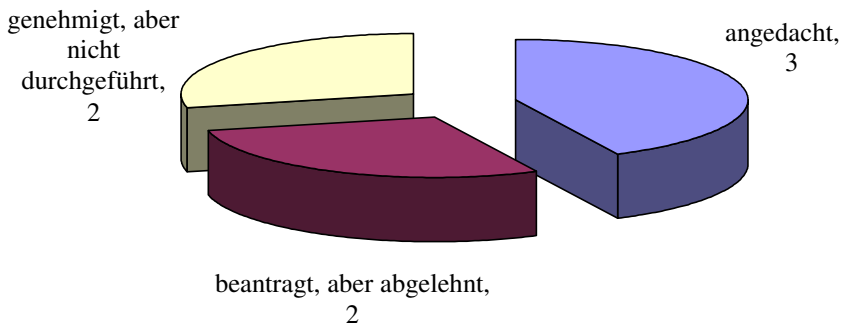
Die **Notwendigkeit einer Online-Durchsuchung** wurde in den ermittlungsrichterlichen Beschlüssen, die vor der erwähnten Entscheidung des BGH vom 31.01.2007 erlassen worden waren und zur Durchführung einer Online-Durchsuchung ermächtigten, unter anderem damit begründet, dass dem Beschuldigten sensibles Datenmaterial in elektronischer Form zur Nutzung auf seinem PC zur Verfügung stehe. Ferner wurde zur Begründung angeführt, geheimdienstliche Strukturen im Ausland sowie Kommunikationswege zwischen dem Beschuldigten und seiner nachrichtendienstlichen Führungsstelle seien durch einen offenen, punktuellen exekutiven Zugriff nicht aufzuklären. Erforderlich sei ein komplexes, zeitlich gestaffeltes Vorgehen, bei dem die verdeckte Durchsuchung der PC-Daten nur einen Teilakt darstelle. Weiter wurde die Notwendigkeit einer Online-Durchsuchung damit begründet, es können sich dadurch

Anhaltspunkte für weitere Ermittlungsmaßnahmen ergeben, ohne den Beschuldigten oder andere Tatbeteiligte vorzuwarnen. Die Ausgestaltung der Online-Durchsuchung als verdeckte Maßnahme ist daher gerade aus polizeitaktischen Gründen notwendig.

3.1.2. Anzahl der Online-Durchsuchungen, Rechtsgrundlagen (vor der BGH-Entscheidung vom 31.01.07) und Verlauf der Verfahren

Eine Online-Durchsuchung wurde - soweit sie dem Projektteam bekannt wurde - lediglich in drei Fällen angedacht und in zwei Verfahren beantragt, aber abgelehnt. In zwei weiteren Fällen wurde die Maßnahme genehmigt, aber nicht durchgeführt. Insofern beziehen sich die Zahlen nicht nur auf die Polizeien des Bundes, sondern auch der Länder.
Nach den im Rahmen des Projekts erlangten Daten wurde daher bislang keine polizeiliche Online-Durchsuchung durchgeführt.

Wurde eine Online-Durchsuchung angedacht, beantragt oder durchgeführt?



Die in der Antwort der Bundesregierung auf eine Kleine Anfrage der Bundestags-Abgeordneten Jan Korte, Petra Pau u.a. vom 28.12.2006[64] erwähnten Beschlüsse des AG Bonn vom 07.02. und 08.11.2006 zu Online-Durchsuchungen liegen dem Projektteam vor. Diese betrafen jedoch – gemessen an der oben genannten Definition – keine Online-Durchsuchung, da in diesen Verfahren mittels eines bekannten Passworts auf Rechner der Beschuldigten zugegriffen werden sollte und der Einsatz einer auf dem Zielsystem zu installierenden Software zum Auslesen von Daten somit nicht erforderlich war. Diese Maßnahmen werden daher in diesem Bericht nicht berücksichtigt. Die dem Verfahren der StA Bonn zu Grunde liegende Konstellation des Zugriffs auf ausgelagerte Daten mittels anderweitig erlangtem Passwort und bekannter Kennung ist in einem ähnlichen Fall

[64] Vgl. BT-Drs. 16/3973, S. 1 f.

Gegenstand in einem anhängigen Verfahren bei dem BVerfG (s. auch Thema 3.3. dieses Projektberichts).

Ebenfalls keine Aufnahme in den Bericht fand eine Maßnahme aus Bayern. Zwar wurde nach Auskunft des bayerischen Staatsministeriums der Justiz[65] in Bayern eine Online-Durchsuchung in einem Ermittlungsverfahren wegen versuchten Mordes durchgeführt. Nähere Erkenntnisse zu diesem Verfahren sind jedoch aus ermittlungstaktischen Gründen nicht mitgeteilt worden und konnten somit auch nicht in den vorliegenden Bericht einfließen.
Die bezüglich dieses Fragekomplexes zugelieferten Fallgestaltungen stellen sich wie folgt dar:

- Die gestellten **Anträge** bzw. erlassenen **Beschlüsse** zur Durchführung einer Online-Durchsuchungen stützten sich zwei Mal auf §§ 102 ff. i.V.m. 100a, b StPO, in einem Fall auf §§ 102, 105 Abs. 1, 94, 98, 169 Abs. 1 Satz 2 StPO und ein weiteres Mal auf §§ 102, 105 Abs. 1, 169 Abs. 1 Satz 2 StPO.
- **Gründe für die Absehen einer polizeilichen Anregung** waren:
  - die Argumentation, dass die Implementierung der Software einen Eingriff in das Wohnungsgrundrecht aus Art. 13 GG darstelle

    > seit BVerfG vom 27.02.08 hinfällig, wobei heute das Recht auf Integrität und Vertraulichkeit Informationstechnischer Systeme zu beachten wäre,
  - die Möglichkeit der Überwachung tatrelevanter verdeckter Kommunikation durch andere Maßnahmen (wie beispielsweise Überwachung des DSL-Anschlusses)

    > Online-Durchsuchung als ultima ratio ggü. einer TKÜ erkannt,

  sowie

  - die Durchführung einer Beschlagnahme des vom Verdächtigen benutzten Laptops während der Durchführung von Reparaturarbeiten,

    > auch hier ultima ratio der Online-Durchsuchung sowie aus taktisch günstiger Gelegenheit anderweitiger Zugriff auf die Daten möglich.

[65] Vgl. Bayerischer Landtag, Landtags-Drs. 15/7502 vom 15.02.2007, S. 4.

- **Gründe für ein Ablehnen der Antragstellung durch die Staatsanwaltschaft zum Erlass eines Beschlusses** stellten sich wie folgt dar:
  - Im konkreten Fall wäre die Maßnahme aus spezifischen Gründen, die hier nicht näher erläutert werden, technisch kaum oder gar nicht möglich gewesen (das Restrisiko des Scheiterns der Maßnahme ist jeder verdeckten Maßnahme immanent) sowie
  - der ablehnende und der Durchführung einer Online-Durchsuchung entgegenstehende Beschluss des BGH vom 31.01.2007 führte zu diesem Zeitpunkt zwingend dazu, von der Beantragung Abstand zu nehmen.
- **Gründe für die Nichtrealisierung eines vorliegenden Beschlusses** zur Durchführung einer Online-Durchsuchung war in zwei Verfahren eine kurzfristig erfolgte Festnahme des Tatverdächtigen, bei dem in einem Fall anschließend im Rahmen offener Maßnahmen u.a. sein Notebook beschlagnahmt werden konnte. Die Gründe für die Nichtrealisierung sind daher der taktischen Lageentwicklung geschuldet.

3.1.3. Anlasstaten

In den Verfahren, in denen eine Online-Durchsuchung nicht nur angedacht, sondern zumindest ein Antrag auf Erlass eines Beschlusses zur Durchführung gestellt wurde, lagen dem jeweiligen Ermittlungsverfahren folgende Straftatbestände zugrunde:

- Verdacht der landesverräterischen und geheimdienstlichen Agententätigkeit,
- Verdacht der Gründung einer terroristischen Vereinigung,
- Rauschgiftschmuggel,
- Bildung einer kriminellen Vereinigung.

Dies zeigt, dass eine Online-Durchsuchung bislang nur in **Fällen von Straftaten von erheblicher Bedeutung, die auch im Einzelfall schwer wiegen,** durchgeführt werden sollte.

3.1.4. Vorausgehende Ermittlungsmaßnahmen

Die typischerweise im Vorfeld einer angedachten Online-Durchsuchung **durchgeführten Ermittlungsmaßnahmen** waren folgende:

- Maßnahmen nach § 100a StPO (bezogen auf Telefon, DSL und E-Mail),

- meist auch eine Verbindungsdatenabfrage,
- eine auch längerfristige Observation.

In Einzelfällen kam es zu:

- einer vorherigen polizeilichen Beobachtung,
- Maßnahmen nach § 100f StPO,
- einem VP- und VE-Einsatz,
- Zeugenvernehmungen,
- einem IMSI-Catcher-Einsatz.

Dies zeigt, dass der Erwägung eine Online-Durchsuchung durchzuführen vielfältige Maßnahmen vorausgingen und die verdeckte Durchsuchung der Festplatte niemals als erster Ermittlungsansatz genutzt werden sollte. Auch vor dem Hintergrund, dass die Online-Durchsuchung eine technisch sehr aufwendige Maßnahme darstellt, die umfangreiche Erkenntnisse hinsichtlich des durch den Tatverdächtigen genutzten Rechners erfordert, wird es sich immer um die ultima-ratio handeln.

3.1.5. Gesetzgeberische Möglichkeiten zur Normierung einer repressiven Ermächtigungsgrundlage

Als gesetzgeberische Möglichkeit zur Regelung einer Online-Durchsuchung wurde in den Expertengesprächen eine explizite Regelung in der **StPO** um eine Befugnis z.B. zur (Zitat in der Zulieferung:) **„Überwachung von Daten“** vorgeschlagen, womit ausschließlich gespeicherte, nicht auf einem Übertragungsvorgang befindliche Daten erfasst werden sollten.[66]

Bei einer gesetzlichen Normierung müsse nach Ansicht der Experten beachtet werden, dass eventuell auch ein physikalischer Zugriff auf den betreffenden Rechner notwendig sei, um erforderliche Software zu installieren. Folglich bestehe das Erfordernis, sofern sich der Rechner in nach Art. 13 GG geschützten Räumlichkeiten befände, ein **verdecktes Betretungsrecht** zum Aufspielen des Programms zu normieren. Die Installation der Software könne nach Einschätzung der Experten in einem solchen Fall im Übrigen auch an einem passwortgeschützten Rechner ohne Kenntnis des Passworts erfolgen (z.B. über einen USB-Stick).

[66] auch Antrag des Freistaates Bayern im Bundesrat: Entwurf eines § 100k StPO, BR-Drs. 365/08; Zustimmung im BR konnte nicht erzielt werden.

Da jede Online-Durchsuchung eine technische Einzelfalllösung erfordere, wäre es nach Auskunft der angehörten Experten sinnvoll, dass die Softwareentwicklung von einer **zentralen Institution** mit entsprechendem Personal und angemessener Finanzierung vorgenommen würde. Zudem könne diese Stelle die Software auch im konkreten Fall zum Einsatz bringen, also die Online-Durchsuchung durchführen.
Für die Entwicklung einer so genannten Remote Forensic Software wurden dem BKA im Rahmen des Programms zur Stärkung der Inneren Sicherheit (PSIS) durch Verfügung des BMI Haushaltsmittel zugewiesen. Diese Software soll nach Fertigstellung eine Basis darstellen, auf der aufbauend im konkreten Einzelfall eine individuell für den betreffenden Rechner passende Konfiguration entwickelt werden kann.

3.1.6. Schranken für die Anwendung der Online-Durchsuchung nach der Rechtsprechung des BVerfG

Das BVerfG entschied am 27.02.2008 über zwei Verfassungsbeschwerden, die unter anderem die Verfassungswidrigkeit des § 5 Abs. 2 Nr. 11 VSG NRW[67] geltend gemacht hatten.[68] Die Vorschrift lautet:

> *„(2) Die Verfassungsschutzbehörde darf nach der Maßgabe des § 7 zur Informationsbeschaffung als nachrichtendienstliches Mittel die folgenden Maßnahmen anwenden:*
>
> …..
>
> *11. heimliches Beobachten und sonstiges Aufklären des Internets, wie insbesondere die verdeckte Teilnahme an seinen Kommunikationseinrichtungen beziehungsweise die Suche nach ihnen, sowie der heimliche Zugriff auf informationstechnische Systeme auch mit Einsatz technischer Mittel.“*

Nach Auffassung der Beschwerdeführer verletzt § 5 Abs. 2 Nr. 11 VSG NRW u.a. das Recht auf Unverletzlichkeit der Wohnung. Viele vertrauliche Informationen, die früher in körperlicher Form in der Wohnung aufbewahrt wurden und damit in den Schutzbereich der Wohnung fielen, würden heute auf dem Computer gespeichert und müssten daher dem Schutzbereich des Art. 13 GG unterfallen. Die Voraussetzungen für die Rechtfertigung eines Eingriffs nach Art. 13 Abs. 2 bis 7 GG lägen nicht vor. Darüber hinaus werde das Recht auf informationelle Selbstbestimmung verletzt, da die Regelung der Online-Durchsuchung weder normenklar noch verhältnismäßig ausgestaltet sei. Soweit § 5 Abs. 2

[67] In der Fassung des Gesetzes zur Änderung des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen vom 20. Dezember 2006, GV. NW 2006, S. 620.
[68] BVerfG NJW 2008, 822 ff.

Nr. 11 VSG NRW ein Beobachten des Internets für zulässig erkläre, werde das Fernmeldegeheimnis verletzt.

Das BVerfG hat § 5 Abs. 2 Nr. 11 VSG NRW mit Urteil vom 27.02.2008 für nichtig erklärt. Allerdings betonte das Gericht, dass mit diesem Urteil keine generelle Entscheidung zur Verfassungsmäßigkeit und Zulässigkeit einer gesetzlichen Ermächtigungsgrundlage zur Durchführung einer Online-Durchsuchung getroffen wurden sei. Dies gelte sowohl für Online-Durchsuchungen zum Zwecke der Strafverfolgung als auch für solche zur Gefahrenabwehr. Vielmehr dürfe der Gesetzgeber grundsätzlich die Online-Durchsuchung als Ermittlungsinstrument einführen, habe aber hohe Voraussetzungen zu normieren.

Insbesondere müsse sich eine gesetzliche Ermächtigungsgrundlage zur Online-Durchsuchung an dem aus Art. 2 Abs. 1 i.V.m. Art. 1 GG ableitbaren und letztlich aus dem allgemeinen Persönlichkeitsrecht resultierenden **Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme** messen lassen. Dieses Schutzgut hat das BVerfG mit der Entscheidung vom 27.02.2008 im Wege der Rechtsfortbildung entwickelt. § 5 Abs. 2 Nr. 11 VSG NRW genüge, so das BVerfG, den insoweit zu beachtenden verfassungsrechtlichen Anforderungen nicht.

Im Einzelnen hat das BVerfG dem Gesetzgeber folgende verfassungsgerichtliche **Vorgaben für die Schaffung einer mit dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme zu vereinbarenden Norm** zur Durchführung von Online-Durchsuchungsmaßnahmen aufgestellt:

- Es müssen tatsächliche Anhaltspunkte für eine konkrete Gefahr für ein überragend wichtiges Rechtsgut wie
  - Leib, Leben und Freiheit der Person oder
  - solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berühren,

  vorliegen.

  Je höher die im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut ist, desto niedriger dürfen die Anforderungen an die Wahrscheinlichkeit des bevorstehenden Schadenseintritts sein.

- Die Anordnung ist grundsätzlich durch den Richter zu treffen. Zudem können zum Schutz der Interessen von Betroffenen weitere verfahrensrechtliche Vorkehrungen erforderlich sein.
- Es müssen hinreichende gesetzliche Vorkehrungen getroffen werden, die Eingriffe in den absolut geschützten Kernbereich privater Lebensgestaltung vermeiden. Der Schutz von Daten höchstpersönlichen Inhalts darf allerdings zweistufig ausgestaltet werden („Zweistufiges Schutzkonzept“):
  - Die Erhebung kernbereichsrelevanter Daten sollte, soweit dies informations- und ermittlungstechnisch möglich ist, von vornherein unterbleiben. Insofern sind verfügbare informationstechnische Sicherungsmechanismen zu nutzen.
  - Ist dagegen eine Bewertung des Kernbereichsbezugs von Daten erst nach Erlangen der Information möglich, so muss dafür gesorgt werden, dass dem Gebot des Schutzes kernbereichsrelevanter Daten in der Auswertungsphase Rechnung getragen wird. Dies bedeutet jedenfalls, dass gewonnene kernbereichsbezogene Daten unverzüglich zu löschen sind und ihre Verwertung ausgeschlossen ist.

Darüber hinaus hat das BVerfG festgestellt, dass eine Online-Durchsuchung **nicht Art. 13 GG** – das Recht auf Unverletzlichkeit der Wohnung – tangiere, soweit keine Erkenntnisse von Peripheriegeräten wie einer Webcam oder eines Mikrofons erlangt werden. Fraglich ist daher, ob ein Recht zum Betreten einer Wohnung zur Installation der erforderlichen Software – als Annexkompetenz einer noch zu schaffenden – Norm angenommen werden kann, wenn allein Eingriffe in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gerechtfertigt werden. Insofern bleibt für den Gesetzgeber bei der Normierung einer Befugnis zur Durchführung einer Online-Durchsuchung zu bedenken, gegebenenfalls explizit ein **Recht zum Betreten von Wohnräumen und anderen Räumlichkeiten zur Installation** der für eine Online-Durchsuchung erforderlichen Software zu normieren und sich nicht darauf zu beschränken, das Aufspielen der Software und die Datenerhebung als solche gesetzlich zu regeln. .

Zudem liegt nach der Entscheidung des BVerfG bei der Durchführung einer Online-Durchsuchung kein Eingriff in Art. 10 GG vor. Denn der Schutz des Fernmeldegeheimnisses erstreckt sich nicht auf die nach Abschluss eines Kommunikationsvorgangs

im Herrschaftsbereich eines Kommunikationsteilnehmers gespeicherten Inhalte und Umstände der Telekommunikation.[69]

3.1.7. Auswirkungen des gegenwärtigen Fehlens einer repressiven Ermächtigungsgrundlage

Als **Auswirkungen des gegenwärtigen Fehlens** einer gesetzlichen Grundlage für die Durchführung von Online-Durchsuchungen wurden sowohl in den Fragebögen als auch in den Expertengesprächen genannt:

- in den meisten Fällen sei noch nicht einmal bekannt, ob und wie die Tatverdächtigen geschlossene Benutzergruppen oder private Postfächer nutzten;
- mögliche Texte mit Bezug zu Anschlägen hätten nicht gesichert werden können;
- es sei zu einem Informationsverlust und damit verbunden zu einer lückenhaften Rekonstruktion von Ereignissen gekommen;
- verschlüsselte auf einem PC gespeicherte Daten hätten nicht ausgewertet werden können. Bei Tatverdächtigen im IuK-Bereich sei es üblich, alles auf dem PC zu speichern. Weitere Beweismittel (schriftliche Vermerke o.ä.) hätten nicht aufgefunden werden können.

3.1.8. Schlussfolgerungen

Nach einhelliger Meinung der befragten Dienststellen ist das Erzielen eines **Ermittlungserfolges** ohne eine Befugnis zur Durchführung von Online-Durchsuchungen in Einzelfällen **erschwert** bzw. **aussichtslos**. Es besteht aus der Sicht der Praxis das dringende Bedürfnis, in besonders gelagerten Fällen eine Ermittlungsmethode zur verdeckten Erlangung von Informationen einsetzen zu können.

Es handelt sich bei der Online-Durchsuchung um eine komplexe technische Maßnahme, deren Erfolgswahrscheinlichkeit von einer Vielzahl technischer Rahmenbedingungen des Einzelfalls abhängig ist. Dennoch erfordern die sich ständig weiter entwickelnde Technisierung der Gesellschaft sowie der bereits durch die Sachverständigen in der Verhandlung am BVerfG dargelegte und durch das BVerfG anerkannte polizeiliche Bedarf die Normierung einer solchen Maßnahme.

[69] Vgl. BVerfG NJW 2008, 822, (825 Rz. 184 f.).

3.1.9. Exkurs zur Quellen-TKÜ

Auch wenn das Thema "Quellen-TKÜ" nicht explizit Gegenstand des Projektes AGNES vorgesehen war, wurde in einigen Zulieferungen und Experteninterviews das im Vergleich zur Online-Durchsuchung allenfalls technisch ähnliche, jedoch rechtlich und taktisch sehr unterschiedlich zu bewertende Instrument der Quellen-TKÜ erwähnt. Der polizeiliche Bedarf, das Instrument der Quellen-TKÜ subsidiär zur konventionellen TKÜ einzusetzen, ist insbesondere angesichts der zu erwartenden zunehmenden Nutzung von Möglichkeiten **kryptierter** Telekommunikation durch das "polizeiliche Gegenüber" hoch.[70]

Unter der so genannten Quellen-TKÜ ist der **verdeckte Zugriff auf Telekommunikationsinhalte** und -daten zu verstehen, die mittels einer „normalen“ TKÜ auch hätten erhoben werden können, dort aber insbesondere aufgrund einer Kryptierung technisch nicht auswertbar sind. Darüber hinaus können auch Telekommunikationsinhalte und -daten bei nomadischer Nutzung eines mittels einer Remote Forensic Software infiltrierten Zielsystems überwacht und aufgezeichnet werden. Der Name Quellen-TKÜ ist darauf zurückzuführen, dass die Gespräche an der „Quelle“ ihrer Entstehung, nämlich bei dem Kommunikationsmittel eines Kommunizierenden (z.B. PC, Kryptohandy, Smartphone), vor der Verschlüsselung (oder nach der Entschlüsselung) zur Überwachung abgegriffen werden.

Hauptanwendungsfall der Quellen-TKÜ ist die Überwachung verschlüsselter Telefonate, die mittels **VoIP** (z.B. mit Skype – standardmäßig verschlüsselt) über das Internet geführt werden. Die gestiegene VoIP-Nutzung[71] wird nach Einschätzung der befragten Experten weiter steigen und die herkömmliche Telefonie über kurz oder lang verdrängen.

Die Quellen-TKÜ ist hinsichtlich der Art des Zugriffsziels klar von der Online-Durchsuchung zu unterscheiden. Bei der Quellen-TKÜ interessieren ausschließlich Kommunikationsdaten, bei der Online-Durchsuchung dagegen auf dem System gespeicherte Daten, die sich nicht (mehr) in einem Kommunikationsvorgang befinden. Rein technisch ist die Vorgehensweise in beiden Fällen zwar durchaus vergleichbar, wobei allerdings bei der Quellen-TKÜ die Art der erhobenen Daten, damit die Zielrichtung eine

[70] h.E. ist die Quellen-TKÜ im Lichte der Vorgaben des BVerfG vom 27.02.08 von der geltenden Rechtslage bereits gedeckt, s. auch §§ 100a, b StPO. Der Richter hat insoweit nach § 100b II StPO u.a. Art und Umfang der Maßnahme darzulegen und insoweit auch den Maßgaben des BVerfG Rechnung zu tragen. Die in § 20 l II BKAG-E vorgesehene explizite Regelung der Quellen-TKÜ hat insoweit h.E. deklaratorische Bedeutung.

andere ist und man daher zu einer unterschiedlichen verfassungs- wie einfachgesetzlichen Bewertung der beiden Instrumente gelangt. Gleichwohl wurden im Rahmen des Projekts AGNES unter dem Themenbereich Online-Durchsuchung auch fünf Fälle zugeliefert, die Quellen-TKÜ-Maßnahmen darstellten. Da im Rahmen des Projekts auch Nachfragen zur Zulässigkeit sowie Durchführung von Quellen-TKÜ-Maßnahmen an KI 15 gerichtet wurden, wird an dieser Stelle im Rahmen eines Exkurses- wie bereits in der vorangestellten Erläuterung bereits dargelegt - näher auf das Thema Quellen-TKÜ eingegangen.

3.1.9.1. Notwendigkeit der Quellen-TKÜ

Eine Überwachung der über VoIP getätigten Telefonate ist durch Ausleitung von den jeweiligen VoIP-Anbietern möglich, sofern die Telefonate nicht **verschlüsselt** sind. Liegt allerdings eine Kryptierung vor, verfügt der Anbieter neben den nicht auswertbaren verschlüsselten Daten in der Regel nur über folgende verwertbare Daten:

- Registrierungsinformationen wie E-Mail-Adresse und IP-Adresse zum Zeitpunkt der Anmeldung (wobei diese Daten beispielsweise auch solche eines Internetcafés sein können);
- Angaben zu gebührenpflichtigen Nutzungen des vorausgegangenen Jahres;
- Anschlussinhaberdaten des Kunden;
- IP-Adresse, wenn finanzielle Transaktionen vorgenommen wurden.

Aufgrund der Struktur von VoIP (abweichende Routen für Signalisierungsinformationen und Verbindungsinhalte) sind die Provider derzeit technisch nicht in der Lage, Verbindungsinhalte **auswertbar** auszuleiten. Für Anbieter mit Erbringung des Dienstes im eigenen (Zugangs-)Netz besteht eine Übergangsfrist bis 01.01.2009, ab der ein rechtsverbindlicher Anspruch auf Ausleitung bestimmter Verkehrsdaten, nicht aber von Telekommunikationsinhalten in unverschlüsselter Form, besteht.

Nur im Kommunikationsmittel des Versenders oder Empfängers sind alle IP-Pakete vorhanden und nicht verschlüsselt. Eine Überwachung der mittels VoIP geführten verschlüsselten Telefonate ist deshalb nur möglich, indem die Kommunikation vor der Verschlüsselung oder nach der Entschlüsselung abgefangen und an die Ermittlungsbehörden weitergeleitet wird. Dies kann durch die Installation einer speziellen

[71] Vgl. Bundesnetzagentur, Jahresbericht 2006, S. 58 f., stetiger Anstieg der Nutzung von VoIP.

Software ähnlich der Online-Durchsuchungs-Software ermöglicht werden. Die Quellen-TKÜ ist deshalb, wie bereits oben erwähnt, mit der Online-Durchsuchung technisch artverwandt. Sie ist allerdings rechtlich von der Online-Durchsuchung völlig zu unterscheiden, da auf Daten auf dem Übertragungsweg zugegriffen wird und die Eingriffstiefe aufgrund des freiwilligen Herausgebens der Daten an einen Kommunikationspartner durch den Betroffenen geringer ist als bei der Online-Durchsuchung.[72] Durch die beiden unterschiedlichen Maßnahmen wird nach den Ausführungen des BVerfG in der Entscheidung vom 27.02.08 in ganz unterschiedliche Grundrechte eingegriffen (Online-Durchsuchung: Art. 2 I i.V.m 1 I GG; Quellen-TKÜ: Art. 10 GG).

Ausgeleitet werden können je nach Konfiguration der Software jegliche verschlüsselte Kommunikationsarten, also beispielsweise mittels VoIP getätigte Telefonate, Chat-Beiträge oder verschlüsselter E-Mail-Verkehr.

In vier der fünf im Rahmen des Projekts bekannt gewordenen Ermittlungsverfahren, bei denen eine Quellen-TKÜ durchgeführt oder zumindest angedacht worden war, konnte festgestellt werden, dass „normale“ Telefonie von den Verdächtigen zunehmend nur für Verabredungen zu Skype-Telefonaten genutzt wird. Die für die Ermittlungsbehörden inhaltlich relevante weitere Kommunikation erfolgt dann ausschließlich über Skype.

3.1.9.2. Rechtsgrundlage

Allen betrachteten Verfahren lag als **Rechtsgrundlage für eine Quellen-TKÜ § 100a StPO**, in einem Fall als Annexkompetenz, zu Grunde.

IP-basierte Kommunikation ist eindeutig Telekommunikation im Sinne von § 100a StPO.[73] Verfassungsrechtlicher Hintergrund des § 100a StPO ist das durch Art. 10 GG geschützte Fernmelde- und Telekommunikationsgeheimnis. Es umfasst den Übertragungsvorgang von Nachrichten, schützt also vor dem Zugriff auf Kommunikationsdaten auf dem Transportweg. Ist der Übertragungsvorgang beendet oder hat er noch nicht angefangen, greift der Schutz von Art. 10 GG nicht ein bzw. sind die §§ 100a ff. StPO nicht einschlägig. Dies hat für die Quellen-TKÜ insofern Bedeutung, als sie nur zulässig ist, wenn der Datenzugriff auf dem Transportweg erfolgt. Andernfalls läge auch ein Eingriff in das Recht auf den

[72] Vgl. BVerfG NJW 2008, 822 ff..
[73] Vgl. *Sankol*, CR 2008, 13 (14).

Schutz der Vertraulichkeit und die Integrität informationstechnischer Systeme vor, so dass zugleich auch die Voraussetzungen für eine Online-Durchsuchung erfüllt sein müssten. Das hat nach Auffassung des Projekteams weiter zur Konsequenz, dass § 100a StPO als Ermächtigungsgrundlage herangezogen werden kann, wenn verschlüsselte Internetkommunikation während der Übertragungsphase abgegriffen wird.

Ein Eingriff in Art. 13 GG findet bei einer Überwachung von VoIP-Gesprächen in der Regel nicht statt, da Gespräche, die innerhalb von durch Art. 13 GG geschützten Räumen geführt werden und Telekommunikation sind, ausschließlich durch das speziellere Grundrecht des Art. 10 GG geschützt werden.[74] Dies gilt für die klassische Festnetztelefonie ebenso wie für die Internettelefonie.

Maßnahmen nach §§ 100a, b StPO sind auch dann statthaft, wenn sie ohne die Mitwirkung Dritter erfolgen, etwa weil die Polizei der Unterstützung durch einen Telekommunikationsdienstleister nicht bedarf, wenn sie durch eigene technische Mittel die Kommunikationsinhalte während des Übertragungsvorgangs ausleiten kann. § 100b StPO erlaubt eine Inanspruchnahme eines Betreibers zur Durchführung der Maßnahme, setzt sie aber nicht tatbestandlich voraus. Die Erwähnung der Verpflichtung des Betreibers im Gesetzestext (und den nachgeordneten Vorschriften TKG und TKÜV) ist allein in der bisherigen regelmäßig technischen Notwendigkeit begründet, Überwachungsmaßnahmen unter Inanspruchnahme eines Dritten (Netzbetreibers) durchführen zu können. Wenn die technische Möglichkeit besteht, eine solche Maßnahme auch ohne die Inanspruchnahme eines Dritten zu realisieren, mindert dies sogar die Eingriffsintensität der Maßnahme, da der Zwangscharakter gegenüber einem Dritten entfällt. Sofern aber die Mitwirkung Dritter tatsächlich erforderlich ist, sind diese nach § 100b StPO verpflichtet mitzuwirken.[75]

---

[74] Vgl. BVerfG NJW 2008, 822 ff.

[75] Anderer Auffassung ist *Sankol*, CR 2008, 13 (15), er argumentiert, bei Maßnahmen nach § 100a StPO müsse auf das Leitungsnetz eines Telekommunikationsunternehmens zugegriffen werden. Ein Zugriff auf das Endgerät des Betroffenen sei von § 100a StPO nicht gedeckt.
Sankol müsste dann aber konsequenterweise auch den Einsatz einer „Wanze“ im Telefonhörer eines Betroffenen zur Überwachung der Telekommunikation als nicht von § 100a StPO umfasst ansehen.
Zwar gibt es einen Beschluss, der erörtert, ob Maßnahmen nach § 100a StPO nur statthaft sind, wenn sie unter Mitwirkung eines Dritten realisiert werden, doch kommt auch dieser Beschluss – allerdings mit kaum tragbarer Argumentation – zu dem Ergebnis, dass Quellen-TKÜ von § 100a StPO gedeckt sind. Die Argumentation dieses Beschlusses wird in diesem Bericht unter „Gründe für die Erforderlichkeit der Maßnahme“ skizziert.
Vgl. Störing, Strafprozessuale Zugriffsmöglichkeiten auf E-Mail-Kommunikation, Berlin 2007, S. 185 f. kommt ebenfalls zu dem Ergebnis, dass eine Inanspruchnahme der Dienstanbieter keine Voraussetzung für einen Eingriff nach § 100a StPO darstellt.

Die Überwachung verschlüsselter Kommunikation sowie die dafür sachnotwendige und typische Vorbereitungs- und Begleitmaßnahme des Aufbringens spezieller Software auf den Rechner des Betroffenen wurde in mehreren Beschlüssen, die vor der Entschediung des Bundesverfassungsgerichts zur Online-Durchsuchung ergangen sind und auf § 100a StPO gestützt wurden, mit folgender Formulierung zugelassen:

> *„… wird … gemäß §§ 100a Nr. 2, 100b StPO die sofortige durchgehende Überwachung und Aufzeichnung der Telekommunikation des Laptops: … Anschlussinhaber: … mit sofortiger Wirkung für die Dauer von … Monaten, ab heute angeordnet."*

oder:

> *„… wird gemäß §§ 100a, 100b StPO die Überwachung und Aufzeichnung der Telekommunikation bzgl. des DSL-Festnetzanschlusses … für die Dauer von … Monaten, beginnend mit dem heutigen Tage, angeordnet. Die Strafverfolgungsbehörden werden ermächtigt, diejenigen Maßnahmen zu treffen, die erforderlich sind, um die Telekommunikation in unverschlüsselter Form zu überwachen und aufzuzeichnen. Gestattet wird zu diesem Zweck auch die Installation einer Überwachungssoftware auf dem Endgerät des Beschuldigten und die Nutzung dieser Software auch im Wege einer Fernsteuerung."*

oder:

> *„I. Die Überwachung und Aufzeichnung der Telekommunikation, die über die DSL-Leitung geführt wird, die an dem ISDN-Anschluss mit den Rufnummern … betrieben wird, ... wird für die Dauer von … Monaten angeordnet. Die unmittelbare Ausleitung umfasst die in diesem Zusammenhang generierten Audiosignale an den beiden in den Räumen … befindlichen, für Internettelefonie eingerichteten … Computer. … Die … Entscheidung beruht zu I. auf § 100a Satz 1 Nr. 1c, Satz 2, § 100b Abs. 1 Satz 1, Abs. 2, § 169 Abs. 1 Satz 2 StPO…"*

oder:

> *„… wird gemäß §§ 100a, 100b StPO in Verbindung mit §§ 112, 113 TKG die Überwachung und Aufzeichnung sämtlicher ein- und ausgehender Kommunikation des nachfolgende benannten analogen DSL-Anschlusses des Beschuldigten, insbesondere der ein- und ausgehende E-Mail-Verkehr, etwaige Kommunikation über Internet-Chat sowie eventuelle Internet-Telefonie (Voice over IP), für die Dauer von … Monaten angeordnet. Die Strafverfolgungsbehörden werden ermächtigt, diejenigen Maßnahmen zu treffen, die erforderlich sind, um die Telekommunikation an den bezeichneten Telefonanschlüssen in unverschlüsselter Form zu überwachen und aufzuzeichnen."*

„Gestattet wird auch die Installation eines Programms zur Entschlüsselung eingehender und ausgehender Daten auf dem Rechner des Beschuldigten."

oder:

„Die Überwachung und Aufzeichnung der Telekommunikation, die über die Anschlüsse … geführt wird, sowie die Überwachung und Aufzeichnung sämtlichen Datenverkehrs, der über den für diese Anschlüsse geschalteten DSL-Kanal geführt wird, einschließlich der über diesen DSL-Kanal geführten Voice over IP-Telefonate, wird für die Dauer von … Monaten angeordnet.. … Zur Umsetzung der Maßnahmen dieses Beschlusses gemäß § 100a StPO wird gestattet, dass auf dem Rechner des Beschuldigten ohne dessen Kenntnis ein Programm installiert wird, das den Inhalt der über das Internet geführten … [Kommunikation] unverschlüsselt ausleitet. … Die … Entscheidung beruht … auf § 100a Satz 1 Nr. 1c, Satz 2, § 100b Abs. 1 Satz 1, Abs. 2, § 169 Abs. 1 Satz 2 StPO…"

Die Gründe dafür, warum in einem Verfahren die Quellen-TKÜ „nur" auf eine **Annexkompetenz** zu § 100a StPO gestützt wurde, lauteten:

„Die Maßnahme ist zudem als Annexkompetenz unter Beachtung der Verhältnismäßigkeit von der Ermächtigungsgrundlage des § 100a StPO gedeckt. § 100a StPO gestattet die Überwachung und Aufzeichnung der Telekommunikation. Diese ist vorliegend nicht möglich, da der Beschuldigte die Daten verschlüsselt versendet. Für das Ergreifen geeigneter Maßnahmen, die verschlüsselten Daten für die Ermittlungsbehörden sichtbar zu machen und so die Überwachung der Telekommunikation überhaupt zu ermöglichen, fehlt es an einer ausdrücklichen Ermächtigungsgrundlage in der StPO. Allerdings sind derartige Maßnahmen unter Rückgriff auf das anerkannte Instrument der Annexkompetenz mit von der Ermächtigung nach § 100a erfasst (vgl. für den Fall des § 100 c Abs. 1 Nr. 1b StPO BGH NJW 01, 1658). Die Vorschrift gestattet den Strafverfolgungsbehörden unter Beachtung des Verhältnismäßigkeitsgrundsatzes auch die Vornahme von notwendigen Begleitmaßnahmen im Vorfeld. Hierzu gehört auch die Installation eines Programms auf dem Rechner des Beschuldigten zur Entschlüsselung der von ihm versandten Telekommunikationsdaten."

Eine Beschränkung des richterlichen Beschlusses ausschließlich auf VoIP (Internet-Telefonie) sollte vermieden werden.

Ein Antrag ist allenfalls dann sinnvoll, wenn verschlüsselte Kommunikation mittels E-Mail, Video oder Chat ausgeschlossen werden kann, da bei einer derartigen Beschränkung beispielsweise eine Ausleitung von „Secure Socket Layer – (SSL)“ Schlüsseln, von Aufnahmen von Sprachkommunikation über den MSN-Messenger und von allen sonstigen verschlüsselten Daten des Programms Skype, die nicht dem Typ VoIP entsprechen, nicht statthaft ist.

Um eine Umgehung des Ermittlungsinstrumentes zu vermeiden, ist bei Beantragung eines Beschlusses darauf zu achten, dass sich dieser auf die von einer Person genutzten informationstechnischen Systeme bezieht und nicht auf veränderbare Angaben wie beispielsweise die Mac-Adresse des Rechners (individuelle Gerätenummer jedes Rechners). Die Individualisierung der betreffenden Person ist dabei durch andere flankierende Maßnahmen sicherzustellen.

In einem Verfahren hat der Softwareanbieter gegenüber der Staatsanwaltschaft bzw. dem Gericht erklärt, dass die Software in ihrer Funktionalität auf VoIP-Anwendungen beschränkt ist. In den anderen Verfahren wurden jeweils besondere gerichtliche **Vorgaben** erlassen, um eine Abgrenzung der Quellen-TKÜ zur (unzulässigen) Online-Durchsuchung sicherzustellen (dies wird nunmehr durch die Entscheidung des BVerfG vom 27.02.08 explizit gefordert):

> *„Dabei ist sicherzustellen, dass auf andere Daten als die zu überwachende Telekommunikation kein Zugriff erfolgt.“*

oder:

> *„Dabei ist sicherzustellen, dass keine Maßnahmen ergriffen werden, mittels derer andere Daten als die zur Telekommunikation übertragenden eingesehen und diese nicht erst nach Beendigung des Übertragungsvorgangs ausgewertet werden.“*

oder:

> *„Ferner ist in der Anordnung klargestellt, dass diese weder den Zugriff auf andere Daten als die zur Telekommunikation übertragenden erlaubt, noch die Ansicht von nach dem Ende des Telekommunikationsvorgangs abgelegten Daten zulässt. Andernfalls würde es sich um einen Fall der so genannten „Online-Durchsuchung“ handeln, bei der auf dem Computer des Beschuldigten oder auf Servern Dritter*

gelagerte Daten zum Zwecke der Ansicht ohne Wissen des Beschuldigten kontrolliert werden. Eine solche Maßnahme wäre nicht zulässig (vgl. BGH NJW 07, 930; BGH Beschluss vom 25.11.2006, 1 BGs 184/2006) und nicht mehr von der Annexkompetenz zu § 100a StPO gedeckt."

Möglich ist auch ein **präventiver Einsatz** von Quellen-TKÜ-Maßnahmen, sofern das jeweilige Landespolizeigesetz Telekommunikationsüberwachungsmaßnahmen zulässt, wie beispielsweise in § 33a des Niedersächsischen SOG. Präventive Quellen-TKÜ-Maßnahmen sind im Rahmen des Projekts AGNES jedoch nicht bekannt geworden.

Die Erforderlichkeit einer Quellen-TKÜ wurde nur beispielhaft in den analysierten Beschlüssen wie folgt begründet:

„… Zur Kommunikation werden neben herkömmlichen Kommunikationsmitteln (Telefon, Mobiltelefon) verstärkt Internetdienste wie ICQ Chat, VOIP bzw. Skype von den Beschuldigten eingesetzt. Aufgrund der vorliegenden Hinweise aus der Telekommunikationsüberwachung ist davon auszugehen, dass der Beschuldigte im Rahmen seiner Kommunikation mit weiteren Tatbeteiligten sowohl Skype als auch erfolgreich VPN Software einsetzt. Bei einer Kommunikation zwischen zwei Skype-teilnehmern findet ein verschlüsseltes Gespräch zwischen den Beteiligten (eine sog. peer-to-peer Kommunikation) statt, das von der eingesetzten Aufzeichnungs- und Überwachungstechnik nicht dargestellt bzw. dekryptiert werden kann. Ebenso wenig ist die TKÜ Anlage in der Lage, über VPN Server geführte verschlüsselte Kommunikation (Telefonie, Chat, Https) interpretierbar (hör- bzw. lesbar) darzustellen. Die Ermittlungsbehörde steht im Kontakt mit einem Anbieter von TKÜ Anlagen, der eine technische Ausgleichsmaßnahme anbietet, mittels derer sowohl Skype Telefonate als auch über VPN verschlüsselte ICQ Kommunikation von dem Rechner des Beschuldigten hör- bzw. lesbar auf eine Auswerteeinheit unbemerkt vom Beschuldigten übertragen werden kann. Zur Durchführung dieser Telekommunikationsüberwachung ist es erforderlich, auf dem Rechner des Beschuldigten unbemerkt eine spezielle Software aufzubringen, die die o.a. Funktionalität (Überwachung der ICQ- und Skype Kommunikation) beinhaltet. Durch die technische Maßnahme werden außer den Telekommunikationsdaten keine weiteren Daten, insbesondere keine auf Datenträgern abgespeicherten Informationen ausgelesen. Eine Beeinträchtigung des Systems im Sinne einer Beschädigung des Dateninhaltes erfolgte nach allgemeiner Abschätzung nicht. Insoweit ist die Maßnahme nicht mit einer Onlinedurchsuchung vergleichbar. Es wird hier nur die Telekommunikation des Rechners konkret aufgezeichnet. Bestehende Daten auf dem System werden nicht ausgelesen. …"

„Die angeordnete Maßnahme ist zur weiteren Sachverhaltsaufklärung erforderlich und geboten, wie die Erforschung des Sachverhalts auf andere Weise wesentlich erschwert, wenn nicht überhaupt aussichtslos wäre."

oder:

„Dabei haben die bisherigen Ermittlungen ergeben, dass der Beschuldigte so genannte Chaträume im Internet benutzt, um mit teilweise noch unbekannten Mitbeschuldigten zu kommunizieren. …"

oder:

„Der Beschuldigte führte seine Voice over IP-Telefonate teilweise unter Verwendung einer Software, die die Gespräche so verschlüsselt, dass ihr Inhalt alleine durch die Überwachung des über den DSL-Kanal geführten Datenverkehrs nicht ermittelt werden kann. Zur Durchführung der Telekommunikationsüberwachung ist es daher erforderlich, auf dem Rechner des Beschuldigten spezielle Software zu installieren, die den Inhalt der über das Internet geführten Telefonate bereits vor deren Verschlüsselung ausleitet. Die hierfür notwendige Rechtsgrundlage findet sich ebenfalls in § 100a StPO. Denn diese Vorschrift gestattet im Wege der Annexkompetenz auch die Vornahme der Begleitmaßnahmen, die für die Umsetzung der Telekommunikationsüberwachung notwendig sind. Solche zur Umsetzung der Maßnahme erforderlichen Begleitmaßnahmen sind auch dann zulässig, wenn sie wie hier mit einem Eingriff in die Eigentumsrechte des Betroffenen verbunden sind, sofern ein anderes, milderes Mittel nicht zur Verfügung steht (vgl. BGHSt 46, 266, 273 f. zur Rechtmäßigkeit von Begleitmaßnahmen bei Maßnahmen nach § 100c Abs. 1 S. 1 Nr. 1b StPO a.F.). So liegt es hier. Denn ohne die Installation des zusätzlichen Programms auf dem Rechner des Beschuldigten kann die Überwachung der über das Internet geführten Telefonate nicht erfolgen. Die Telekommunikationsüberwachungsmaßnahme wäre mithin nicht möglich. Der Anordnung steht auch nicht entgegen, dass der Gesprächsinhalt der verschlüsselten Telefonate nach der Installation des Programms ohne Beteiligung der Netzbetreiber an die Ermittlungsbehörden ausgeleitet wird. Zwar wird in der Kommentarliteratur überwiegend die Auffassung vertreten, § 100a StPO räume den Ermittlungsbehörden nicht die Befugnis ein, Telekommunikation ohne Zutun eines Netzbetreibers zu überwachen (L/R-Schäfer, 25. Aufl., § 100a Rn. 9 und 31 f.; Meyer-Goßner, 50. Aufl., § 100a Rn. 2; KK-Nack, 5. Aufl. § 100a Rn. 5; so auch Gercke CR 2007, 245, 252). Selbst wenn man dieser Auffassung folgt, ergibt sich hieraus aber nicht die Unzulässigkeit der hier beantragten Maßnahme. Denn vorliegend erfolgt die Überwachungsmaßnahme nicht unter Ausschluss der Netzbetreiber. Vielmehr wird diesen ebenfalls aufgegeben, die in ihrem Herrschaftsbereich anfallenden Daten an die Ermittlungsbehörden auszuleiten. Diese Daten des Netzbetreibers sind im entschlüsselten Zustand mit den Daten identisch, die

mittels des auf dem Rechner des Beschuldigten installierten Programms ausgeleitet werden. Im Ergebnis dient die Maßnahme mithin nur der Entschlüsselung der auch beim Netzbetreiber anfallenden Daten (für die Zulässigkeit der Maßnahme auch Bär, Handbuch zur EDV-Beweissicherung im Strafverfahren, Rn. 318 m.w.N.).“[76]

3.1.9.3. Schlussfolgerungen

In mehreren Ermittlungsverfahren wurden Beschlüsse zu Quellen-TKÜ-Maßnahmen auf der Basis des § 100a StPO erlassen. Diese Norm ist wurde vor der Entscheidung des Bundesverfassungsgerichts zur Online-Durchsuchung von den Gerichten als ausreichende Ermächtigungsgrundlage zur Durchführung von Quellen-TKÜ-Maßnahmen angesehen.

Unter anderem richtete sich somit der Kernbereichsschutz nach § 100a Abs. 4 StPO.[77]

Sofern in einem Ermittlungsverfahren bekannt wird, dass verschlüsselte Kommunikation stattfindet, sollte die Durchführung einer Quellen-TKÜ in Betracht gezogen werden.

[76] Diese Argumentation dürfte allerdings nicht tragfähig sein: Denn bei einer Quellen-TKÜ erlangt die Polizei alle erforderlichen Daten bereits durch den Zugriff auf den Rechner des Betroffenen. Einer Mitwirkung des Dritten bedarf es gerade nicht. Anders als der Beschluss suggeriert, ist ein Vergleich der über den Zugriff auf den Zielrechner erlangten Daten mit den verschlüsselten Daten, die über den Provider erlangt werden könnten, nicht erforderlich. Die über den Provider theoretisch erhältlichen verschlüsselten Daten sind für die Polizei ohne jegliche Relevanz.

[77] Vgl. Urteil des BVerfG NJW 2008, 822 ff.

3.2. Verdeckte Teilnahme an geschlossenen Chats

Unter der verdeckten Teilnahme an geschlossenen Chats wird im Rahmen dieses Projekts die Beteiligung an einem zugangsgeschützten Chat durch die Polizei unter Nichtoffenlegung des polizeilichen Zwecks der Teilnahme verstanden.

Als offen wird ein Chat bezeichnet, wenn **keine wirksamen**, auf einen eng begrenzten Adressatenkreis ausgerichteten **Zugangsbeschränkungen** erkennbar sind. So bewirkt nach Ansicht der befragten Experten z.B. das Veröffentlichen des Zugangspassworts zu einem mit dem Internet verbundenen Rechner in einem Forum mit Hunderten unbekannter anderer Teilnehmer grundsätzlich eine Öffentlichkeit dieses Angebots. Ebenso zu bewerten seien Zugangsschranken bei kommerziellen Angeboten - wie etwa das Abfragen von Kreditkarten- und Ausweisdaten – die nur auf die geschäftsmäßige Abwicklung der Chatraum-Nutzung oder den Nachweis der Volljährigkeit eines Nutzers abzielen.[78]

Von besonderem Interesse ist für diesen Themenbereich, welche Rechtsgrundlage für eine Chat-Teilnahme als einschlägig erachtet wird und welche konkreten Maßnahmen zur Erkenntnisgewinnung erforderlich sind.

Für den Bericht wurden vier Fragebögen sowie fünf Expertengespräche zur verdeckten Teilnahme an geschlossenen Chats ausgewertet. Im Folgenden werden die auf dieser Basis gewonnenen zentralen Erkenntnisse dargestellt.

3.2.1. Anzahl der Chatteilnahmen sowie Alternativmaßnahmen

In nur zwei Fällen kam es zu einer Teilnahme an einem Chat, in zwei weiteren Verfahren wurde eine solche Maßnahme nur geplant, aber letztlich nicht durchgeführt.

Von den beiden geplanten Maßnahmen wurde eine schon beschlossene Chat-Teilnahme aus zeitlichen Gründen nicht realisiert.

[78] *Kudlich*, JA 2000, 227 (229) argumentiert ebenfalls, dass generalisierte Abfragen, etwa des Alters eines Teilnehmers oder dessen Kreditkartennummer, nicht zu einer Eingrenzung des Personenkreises eines Chats auf ausgewählte Teilnehmer führen.

Die geringe Anzahl von Teilnahmen an geschlossenen Chats lässt sich damit erklären, dass im Rahmen einer DSL-Überwachung auf der Grundlage von § 100a StPO die Kommunikation innerhalb eines Chats ausgeleitet werden kann, so dass eine Teilnahme an dem Chat selbst überhaupt nicht erforderlich ist. Eine solche Ausleitung funktioniert nur dann nicht, wenn innerhalb des Chats verschlüsselt kommuniziert wird, was nach Auskunft eines Experten in ca. 20 % der DSL-Ausleitungen von Chats der Fall ist.

Die der Chatteilnahme vorausgehenden Ermittlungsschritte waren in fast allen betrachteten Fallgestaltungen Überwachungsmaßnahmen gemäß § 100a StPO. In Einzelfällen aber auch Maßnahmen nach § 163f StPO und § 100g StPO.
Anhaltspunkte für eine Förderlichkeit einer Teilnahme für das jeweilige Ermittlungsverfahren ergaben sich in den untersuchten Fällen aus einer TKÜ, einer VP-Aussage bzw. bei einer verdachtsunabhängigen Teilnahme aus dem Namen des Chats.

Eine Überwachung von Inhalten geschlossener Chats **ohne TKÜ** (also ohne TKÜ "im klassischen Sinne", die wegen der Kryptierung ins Leere liefe) ist der Polizei nur nach Anmeldung im Chat oder durch eine Überwachung des Internetservers, über den die Kommunikation des Chatrooms läuft, möglich.

3.2.2. Rechtsgrundlagen

Als Rechtsgrundlage für die verdeckte Teilnahme an einem geschlossenen Chat im Rahmen eines Ermittlungsverfahrens wurde in allen für diesen Bericht ausgewerteten Fällen **§ 100a StPO** herangezogen.

Das BVerfG hat mit Urteil zum § 5 des Verfassungsschutzgesetzes Nordrhein-Westfalen vom 27.02.2008[79] einen Eingriff in Art. 10 GG und damit das Erfordernis von § 100a StPO als Ermächtigungsgrundlage verneint, wenn ein Teilnehmer eines geschlossenen Chats seinen Zugang freiwillig zur Verfügung stellt. Ebenso liege kein Eingriff in das Telekommunikationsgeheimnis vor, wenn allgemein zugängliche Inhalte erhoben würden, etwa in offenen Diskussionsforen oder auf nicht zugangsgesicherten Websites. Werde dagegen ein Passwort zu einem Chat mittels anderer verdeckter Maßnahmen z.B. Keylogging für die Ermöglichung der laufenden Kommunikationsüberwachung erlangt, liege ein Eingriff in Art. 10 GG vor.

[79] Vgl. BVerfG NJW 2008, 822 ff.

Dagegen wurden nach Projektergebnissen auch die Ermächtigungsnormen zum **Einsatz eines Verdeckten Ermittlers, also die §§ 110a ff. StPO,** insoweit nicht für einschlägig erachtet bzw. angewandt als eine dauerhaft angelegte, legendierte Teilnahme in Form einer aktiven Täuschung der Chatteilnehmer erfolgte.
Daraus ergibt sich, dass ohne eine solche Legendierung die Teilnahme an einem geschlossenen Chat aufgrund der Generalklausel nach §§ 161, 163 StPO erfolgen kann.

Eine verdeckte Chat-Teilnahme **im Rahmen präventiv-polizeilichen Handelns zur Gefahrenabwehr** ist ebenfalls möglich, beispielsweise nach § 30 Abs. 2 Nr. 4 Niedersächsisches SOG (Regelung zur Ermöglichung einer verdeckten Datenerhebung; Ausnahme zur im Übrigen offenen Datenerhebung). Im Rahmen des Projekts wurden jedoch ausschließlich Fallkonstellationen berichtet, bei denen es sich um repressives polizeiliches Tätigwerden handelte.

3.2.3. Verhalten im Chat

Probleme bei der **Anmeldung** in einem Chat ergaben sich in den betrachteten Fällen sowie nach Aussage der Experten wegen fehlender Kenntnis des Zugangspasswortes oder fehlender, zum Zugang erforderlichen Einladung.

Nach den im Projekt erlangten Erkenntnissen erfolgte im Chat eine **Beobachtung** des Verhaltens der anderen Chat-Teilnehmer. Dabei konnten oftmals Gefahrenlagen erkannt und Hinweise auf Straftaten entdeckt werden.
Zudem mussten gelegentlich auch **Fragen beantwortet** werden. Nach der Polizeizugehörigkeit wurde zumeist nicht gefragt. In Einzelfällen gewährte der Administrator des Chats trotz positiver Bestätigung der Polizeizugehörigkeit Zugang zum Chat.
Ferner wurden Screenshots gefertigt, Inhalte gespeichert sowie pdf-Ausdrucke erstellt sowie Einträge in offenen Bereichen „geposted“. Als problematisch wird nach Auskunft der Experten das Sichtbarsein des Überwachers im Chat erachtet, da hierdurch Misstrauen erweckt werden kann. Wichtig sei daher ein **plausibles Erscheinen und Anpassen an das allgemeine Verhalten** in dem jeweiligen Chat.

Im **Anschluss** an die Chatteilnahme erfolgten üblicherweise eine Durchsuchung, eine Sicherstellung von E-Mails sowie die Sicherstellung von PC und deren Auswertung.

Die **Erkenntnisse aus der Chatteilnahme** wurden in den untersuchten Fällen im Wege des Zeugenbeweises, also der Vernehmung des Recherchebeamten, oder aber einer Protokollverlesung in die betreffenden Gerichtsverfahren eingeführt.

3.2.4. Schlussfolgerungen

Die geringe Anzahl von Zulieferungen erklärt sich dadurch, dass die **Erkenntnisse**, die aus einer Chatteilnahme erlangt werden können, auch im Wege der Ausleitung einer DSL-Überwachung im Rahmen einer repressiven TKÜ nach § 100a StPO gewonnen werden können. Ausgeleitet werden bei einer solchen TKÜ alle Informationen, die der Betroffene aus dem Internet abruft oder über das Internet versendet. Die Kenntnis eines Passworts oder der Zugang zu dem geschlossenen Chat ist hierbei nicht erforderlich.

Das Gleiche gilt für Internetkommunikationsplattformen wie PALTALK, Yahoo-Messenger, ICQ oder Microsoft Messenger. **Probleme** mit dieser Art der Überwachung gibt es nur bei verschlüsselter Kommunikation. Denn in solchen Fällen kann bei einer TKÜ nur festgestellt werden, dass kommuniziert wird, der Inhalt der Unterhaltung ist jedoch nicht zu erkennen.

In den untersuchten Fällen wurde von den betreffenden Dienststellen ausnahmslos § 100a StPO als einschlägige Ermächtigungsgrundlage für die verdeckte Teilnahme an einem geschlossenen Chat erachtet.

Die Teilnahme an einem Chat ist eine offenbar selten genutzte Ermittlungsmaßnahme, die technischen Möglichkeiten sind weitgehend unbekannt. Anlassunabhängige Recherchestellen nehmen nur an offenen Chats teil. Teilnahme an zugangsbeschränkten Chats erfolgt nur dann, wenn das Passwort bekannt ist. Ausweislich der zugelieferten Fallzahlen erfolgt in Ermittlungsverfahren zumeist eine DSL-Ausleitung. Eine Chatteilnahme dagegen nur in Ausnahmefällen in Betracht gezogen.

3.3. Verdeckter Zugriff auf zwischengespeicherte Daten

Im Rahmen des Projekts wird unter einem Zugriff auf zwischengespeicherte Daten verstanden, dass ohne zwingende Mitwirkung eines Netzbetreibers auf Daten zugegriffen wird, die weder unmittelbar beim Absender der Daten noch beim Empfänger gespeichert sind. Unter diesen Voraussetzungen werden beispielsweise Fallkonstellationen erfasst, bei denen ein Zugriff auf

- E-Mails weder beim Empfänger noch beim Absender der E-Mails,
- zugangsgeschützte Speichermöglichkeiten im Internet wie Webspace oder Nethosting,
- Daten in einem für Entwürfe-Ordner eines E-Mail-Postfachs, für das mehrere Personen zugriffsberechtigt sind,

erfolgt.

Von besonderem Interesse ist auch bei dieser Thematik die von den Ermittlungsbehörden in Erwägung gezogene bzw. angewandte Rechtsgrundlage. Zur Frage der Vereinbarkeit eines offenen Zugriffs auf zwischengespeicherte Daten mit dem Grundgesetz ist derzeit beim BVerfG eine Verfassungsbeschwerde anhängig, über die aber bisher außer im Verfahren des einstweiligen Rechtsschutzes noch nicht entschieden wurde.[80] Die anhängige Verfassungsbeschwerde wird voraussichtlich Klarheit bringen können.

Für diesen Bericht wurden 13 Fragebögen sowie zwei Expertengespräche zum verdeckten Zugriff auf zwischengespeicherte Daten ausgewertet. Im Folgenden werden die so gewonnenen zentralen Erkenntnisse dargestellt.

3.3.1. Vorausgehende Ermittlungsmaßnahmen

Von der Existenz zwischengespeicherter Nachrichten haben die Ermittlungsbehörden in den 13 analysierten Fällen auf sehr unterschiedliche Art erfahren: In vier Verfahren erlangten sie aus einer bereits laufenden TKÜ nach §§ 100a, b StPO Anhaltspunkte auf zwischengespeicherte Daten. Bei anderen Fällen erfuhren die Behörden von der Existenz zwischengespeicherter Daten aufgrund eines Hinweises auf verschleierte Absprachen zwischen Tatbeteiligten, einer Zeugenaussage sowie durch eine Observation.

[80] Vgl. hierzu unter 3.3.6.

In zehn von den 13 betrachteten Verfahren ging dem Zugriff eine TKÜ-Maßnahme voraus, in fünf Verfahren wurden zuvor (längerfristige) Observationen, in je drei Verfahren Maßnahmen nach §§ 100g, h StPO a.F.[81] bzw. Vernehmungen durchgeführt.

In Einzelfällen erfolgte der verdeckte Zugriff im Anschluss an

- eine Maßnahme nach § 100i StPO,
- eine Überprüfung durch das Rechnungsprüfungsamt,
- ein Auskunftsersuchen bei einem Provider sowie
- im Nachgang zu allgemeinen Fahndungsmaßnahmen.

Aus den Expertengespächen geht hervor, dass die Erkennntis von der Kontaktaufnahme der Beschuldigten meist im Rahmen einer TKÜ erlangt wurde, da diese das gemeinsame Passwort zu dem Speicherort per Telefon austauschten.

In einem der Beschlüsse, welche die Überwachung eines Entwürfeordners eines E-Mail-Accounts anordneten, wurde folgende Begründung für die Maßnahme angegeben:

> *„… Den konventionellen E-Mail-Verkehr umgeht er dadurch, dass er Informationen in den „Entwurfsordner“ von E-Mail-Accounts ablegt, die dort von seinen Kontaktpersonen nach Aufrufen des Accounts sowie Verwenden desselben Kennworts gelesen und durch Verändern, Ergänzen oder Einstellen eines neuen Textes beantwortet werden.“*

3.3.2. Rechtsgrundlagen

Erlassen wurden Beschlüsse zum **Zugriff auf zwischengespeicherte Daten** unter Heranziehung folgender Rechtsgrundlagen:

- in vier der betrachten Verfahren auf der Basis der Vorschriften nach §§ 100a, b StPO,
- in drei Fällen unter Heranziehung der Beschlagnahmenormen der §§ 94, 98 StPO,
- ein Mal auf §§ 100a, b, g, h StPO,
- ein Mal auf der Basis der §§ 100a, 100 Abs. 1, 2, 100g, h, 169 StPO,

[81] Zum Zeitpunkt der Durchführung der Erhebung war die Neuregelung der StPO durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21.12.2007 (BGBl. 2007 I S. 3198) noch nicht in Kraft getreten. Im Folgenden wird daher auf die §§ 100g, h StPO a.F. Bezug genommen.

- ein Mal auf eine Kombination der Rechtsgrundlagen §§ 100a, b, 94, 98 StPO,
- ein Mal auf § 100a, §§ 100g, h, §§ 94, 98 StPO.

Darüber hinaus wurden in Einzelfällen die §§ 161, 95 StPO, §§ 100g, h StPO sowie der § 99 StPO als Ermächtigungsgrundlagen in Betracht gezogen. In einem der analysierten Fälle wurde keine besondere Rechtsgrundlage für erforderlich erachtet.

Zusammenfassend lässt sich festhalten, dass in der Mehrzahl der Verfahren ein Beschluss unter Heranziehung der TKÜ-Vorschriften erging, während die Beschlagnahmenormen lediglich in vier Fällen herangezogen und in nur einem Verfahren beide Normenkomplexe für einschlägig erachtet wurden.

In einem Beschluss wurde die Anordnung der Überwachung eines E-Mail-Accounts, dessen Entwürfe-Ordner für einen Nachrichtenaustausch genutzt wurde, wie folgt formuliert:

> *„… wird gemäß § 100a Satz 1 Nr. 1c, Satz 2, § 100b Abs. 1 Satz 1, Abs. 2, § 169 Abs. 1 StPO die Überwachung und Aufzeichnung des unter dem Benutzernamen „…" über das E-Mail-Konto … Anmelder: … Provider: … im … Programm geführten Nachrichtenverkehrs für die Dauer von … Monaten beginnend mit dem Zeitpunkt der Anordnung gestattet."*

In einem anderen Beschluss hieß es:

> *„Der hiesige Beschluss vom … [gem. § 100a StPO] wird klarstellend dahingehend ergänzt, dass die zu überwachende und aufzuzeichnende Telekommunikation auch die in den Entwurfsordner des zu überwachenden E-Mail-Accounts eingestellten Daten umfasst.*

Die rechtliche Begründung lautete in einem der Beschlüsse wie folgt:

> *„Der Begriff „Telekommunikation" im Sinne der §§ 100a ff. StPO umfasst grundsätzlich den gesamten Datenverkehr mittels Telekommunikationsanlagen (BGH NStZ 2003, 668 – Urt. vom 14.3.2003, 2 StR 341/02). Entscheidend für die Frage, welche Daten dem Schutz des Fernmeldegeheimnisses – und damit andererseits dem Zugriff im Rahmen einer TKÜ-Maßnahme nach § 100a StPO – unterliegen, ist allein die Frage, ob sich die Daten noch oder wieder im Herrschaftsbereich des Kommunikationsteilnehmers befinden oder außerhalb der Sphäre des Betroffenen, wo sie dem erleichterten Zugriff Dritter ausgesetzt sind (BVerfG Urt. vom 2. März 2006, 2 Bv 2099/04, Rdnrn. 75-77). Durch die Übermittlung einer Nachricht an den bei dem Provider angesiedelten Entwurfsordner hat die Nachricht die Sphäre des Verfassers*

verlassen. Sie unterliegt dem besonderen Schutz des Fernmeldegeheimnisses und damit – als Telekommunikation – den Überwachungsmöglichkeiten der §§ 100a ff. StPO.“

In einem der geführten Interviews gab die Expertin die Regelung der Postbeschlagnahme nach § 99 StPO als einschlägige Ermächtigungsgrundlage an.. Nach einer weiteren Aussage in einem Expertengespräch wurde wie folgt rechtlich differenziert: Die Ausleitung durch den Provider habe nach § 100a StPO, eine Account-Beschlagnahme dagegen nach §§ 94, 98 StPO zu erfolgen.
Einschränkende **Auswirkungen auf die Datenauswertung** hatte ein Beschluss, der auf der Grundlage des § 99 StPO beantragt worden war, jedoch nach §§ 94, 98 StPO erging. Hier konnte eine einmalige Auswertung des E-Mail-Postfachs durchgeführt werden.

In einem weiteren Beschluss wurde danach differenziert, ob die Nachrichten zum Zeitpunkt des polizeilichen Zugriffs bereits **gelesen** oder noch **ungelesen** waren. In Bezug auf gelesene Nachrichten wurden die §§ 94, 98 StPO, bei den ungelesenen E-Mails § 100a StPO als Ermächtigungsgrundlage angewandt.

Nach Ansicht des Projektteams ist die für einen Zugriff aufgrund von Erkenntnissen aus offenen Maßnahmen einschlägige Ermächtigungsgrundlage die Befugnisnorm zur Beschlagnahme von Daten. Einschlägig sind mithin die **§§ 94, 98 StPO**.
Wird beispielsweise bei einer Durchsuchung nach § 102 StPO ein Passwort in Erfahrung gebracht, dass einen Zugriff zu verschlüsselten Daten ermöglicht, die auf einem vor Ort stehenden PC gespeichert sind, so darf bereits aufgrund des Durchsuchungsbeschlusses auf die Computerdaten zugegriffen werden, sofern diese als solche vom Beschluss umfasst sind. Die Richtigkeit dieser Argumentation kann durch folgende Kontrollüberlegung bestätigt werden: Findet man im Rahmen einer Wohnungsdurchsuchung einen Schlüssel zu einem Safe, der sich in der Wohnung befindet und ohne den Schlüssel nicht geöffnet werden kann, darf die Polizei ohne Zweifel den Safe mit dem gefundenen Schlüssel öffnen und die Durchsuchung auch auf die im Safe befindlichen Gegenstände erstrecken, sofern nicht der Safe und sein Inhalt ausdrücklich von dem Durchsuchungsbeschluss ausgeschlossen sind..

Inwieweit die in einem Expertengespräch vorgebrachte Kritik an der Verwendung der Ermächtigungsgrundlage §§ 94, 98 StPO, die nur zum einmaligen Zugriff berechtigen, greift, hängt entscheidend von der Ausgestaltung der Anordnung durch das Gericht ab.

Dass die den offenen Maßnahmen folgende Beschlagnahme auf zwischengespeicherte Daten verdeckt erfolgt, widerspricht einer Anwendung der §§ 94, 98 StPO h.E. nicht. Denn im Gegensatz zu den Durchsuchungsnormen finden sich bei den Beschlagnahmevorschriften keinerlei Vorgaben, die eine Anwesenheit des Beschuldigten bzw. Zeugen sichern sollen und damit ein offenes Vorgehen gebieten. Wird auf die Daten im Rahmen einer Durchsuchung zugegriffen, erfolgt dies nicht verdeckt. Wird der Zugriff dagegen zu einem späteren Zeitpunkt bzw. nicht von den Räumen des Beschuldigten aus realisiert, ist er zwar verdeckt, die §§ 94, 98 StPO differenzieren aber nur nach dem Beweismittel und nicht, in welchem Zusammenhang es erlangt wurde.

Die Daten, auf die jeweils zugegriffen werden soll, befinden sich nicht auf einem Übertragungsweg im Rahmen eines Kommunikationsvorgangs, weshalb die **§§ 100a ff. StPO nicht** einschlägig sind. Die Daten sind gerade nicht für den Versand vorgesehen; auch wenn die Zwischenspeicherung lediglich der Umgehung von Überwachungsmaßnahmen dient, sind sie nicht Teil eines Telekommunikationsvorgangs. Die Gefahr, vor der Art. 10 GG schützen soll, dass von den Daten Kenntnis erlangt wird, da durch die Mitwirkung Dritter beim Transport der Nachricht ein erleichterter Zugriff auf diese möglich ist, besteht insofern nicht.

3.3.3. Realisierung der Beschlüsse

Kenntnis vom Inhalt der zwischengespeicherten Nachrichten auf der Basis der ergangenen Beschlüsse konnte in fünf der 13 analysierten Fälle durch eine Ausleitung der Daten im Auftrag der Polizei vom Provider erlangt werden. In zwei Verfahren ermittelte man zunächst die Zugangsdaten (Benutzerkennung, Passwort) über eine TKÜ und nahm anschließend Einsicht in das E-Mail-Postfach. Bei einem Fall wurde von dem Provider ein Gastzugang freigeschaltet, über den der Zugriff auf die zwischengespeicherten Daten gelang.

Ein Antrag, der sich auf eine Beschlagnahme von E-Mail-Entwürfen bezog, wurde vom zuständigen Gericht **abgelehnt.** Grund hierfür war, dass der Provider nicht zusagen konnte, den Betroffenen nicht von der Maßnahme zu informieren. Diese Maßnahme wurde folglich nicht umgesetzt.

Probleme hinsichtlich der **Mitwirkung des Providers** ergaben sich bei den untersuchten Verfahren im Bereich der Erhebung von Bestandsdaten bei einem Provider. T-Online verweigerte eine Erteilung von Auskünften zu dynamischen IP-Adressen auf der Grundlage von § 113 TKG. In einem weiteren Fall war es dem Provider aufgrund technischer Probleme nicht möglich die Daten mitzuteilen. Darüber hinaus wurden in einem weiteren Verfahren die Inhalte der E-Mail-Konten in Paketen und dadurch mit erheblichem Zeitverzug übermittelt. Der Internetserviceprovider GMX weigerte sich zunächst gänzlich eine Ausleitung der im Entwürfe-Ordner gespeicherten E-Mails vorzunehmen.

Auf die zwischengespeicherten Daten wurde in den untersuchten Fällen in der Regel **mehrmals zugegriffen**. Die Spanne reicht von nur einmaligen Zugriffen in zwei Verfahren bis hin zu fünf Zugriffen am Tag bzw. Zugriffen nach jeder erfolgten Anmeldung durch den Beschuldigten.

Die Frage, wo sich das Speichermedium zum Zeitpunkt des Zugriffs befand, wurde dem Projektteam in elf der betrachteten Fälle beantwortet. Das **Speichermedium**, auf das Zugriff genommen werden sollte, befand sich danach überwiegend – und zwar in acht Fällen – im Inland und in zwei Mal im Ausland. Dies hatte ein langwieriges Verfahren zur Erlangung der Daten mittels Rechtshilfe zur Folge. In einem weiteren Fall war der Standort des Servers unbekannt.

Als **sonstige Probleme** bei einem verdeckten Zugriff auf zwischengespeicherte Daten wurden von den Dienststellen

- eine zu geringe Kapazität des zum Empfang der gespiegelten Daten eingerichteten E-Mail-Kontos,
- fehlende Vorgaben für die Datensicherung und Endarchivierung sowie
- das Fehlen einer sicheren Datenverbindung zwischen dem Provider und den Sicherheitsbehörden

genannt.

3.3.4. Verwertung der Erkenntnisse

Die durch einen verdeckten Zugriff erlangten Erkenntnisse führten nach deren Auswertung in je zwei Fällen zu Vernehmungen, Durchsuchungen, vorläufigen Festnahmen sowie

Fahndungsmaßnahmen. In einem untersuchten Verfahren stand der Zugriff auf die zwischengespeicherten Nachrichten zum Zeitpunkt des Projektabschlusses noch aus. Ein Fall wurde gegen Zahlung einer Geldbuße eingestellt. In einem Verfahren wurde der Erlass eines Beschlusses abgelehnt.

In **Gerichtsverfahren** wurden die durch einen Zugriff auf zwischengespeicherte Daten erlangten Erkenntnisse in drei Fällen im Wege der Protokollverlesung eingebracht, in einem Fall durch Zeugenbeweis.

3.3.5. Alternativmaßnahmen

Alternative Ermittlungsmaßnahmen an Stelle eines verdeckten Zugriffs auf zwischengespeicherte Daten standen nach Auskunft der ermittelnden Dienststellen in der Regel nicht zur Verfügung. In einem Fall wäre ein Zugriff auf Grund von § 100a StPO als Ermächtigungsgrundlage nicht möglich gewesen, da keine Katalogtat vorlag. Allerdings wurde als mögliche Alternative für einen verdeckten Zugriff auf zwischengespeicherte Daten die DSL-Überwachung des Anschlusses genannt, von dem aus der Zugriff auf das betreffende Postfach in der Regel erfolgte.

3.3.6. Offener Zugriff auf Nachrichten

Die rechtliche Einordnung von Nachrichten, die zwar im E-Mail-Account des Empfänger eingegangen, aber noch nicht auf seinen PC heruntergeladen worden sind, ist Gegenstand einer derzeit vor dem BVerfG anhängigen Verfassungsbeschwerde.[82] Streitgegenstand ist hier die Frage, ob eine Beschlagnahme von ca. 2.500 E-Mails des Beschwerdeführers auf seinem Web-Account aufgrund von §§ 94, 98 StPO zulässig war oder es – wie der Beschwerdeführer behauptet – für die Maßnahme eines Beschlusses nach § 100a StPO bedurft hätte.

Seit einer Entscheidung des BVerfG aus dem Jahr 2006 ist geklärt, dass der Schutz des Telekommunikationsgeheimnisses endet, sobald die Information im Herrschaftsbereich des Empfängers angekommen ist.[83] Die spezifischen Gefahren der räumlich distanzierten Kommunikation bestehen dann nicht mehr, da der Empfänger eigene Schutzmaßnahmen gegen einen ungewollten Zugriff auf die Daten ergreifen kann.

[82] 2 BvR 902/06.
[83] BVerfG NJW 2006, 976 ff.

Das AG Braunschweig sowie das LG Braunschweig als Beschwerdeinstanz[84] waren in dem **beim BVerfG anhängigen Verfahren** der Ansicht, dies gelte auch für einen Web-Account, wenn Nachrichten nach erfolgtem Abruf durch den Empfänger auf dem Mail-Server verbleiben und dort nicht gelöscht werden. Das LG Braunschweig formulierte dies im Beschwerdeverfahren wie folgt:

> *„Vorliegend besteht die Besonderheit, dass die E-Mails bestimmungsgemäß nicht auf dem Endgerät des Betroffenen, sondern dem Betroffenen auf einem Speicherplatz beim Provider zur Verfügung gestellt werden. Nach Ansicht der Kammer ist die Situation des Teilnehmers bei endgültiger Speicherung auf einem auswärtigen Speicherplatz bei seinem Provider aber ohne weiteres vergleichbar mit der Speicherung auf einem beim Teilnehmer selbst bereitgestellten Endgerät."*

Die Fragestellung, die das BVerfG in diesem Verfahren in der Hauptsache zu beantworten hat, lautet nach Auskunft des BVerfG wie folgt:
Wird durch den Zugriff auf E-Mails, die auf dem Server eines Kommunikationsunternehmens oder Serviceproviders gespeichert sind, in Art. 10 GG eingegriffen und wenn ja, reichen §§ 94, 98 StPO als Ermächtigungsgrundlage aus? Diese Frage sei, so das BVerfG, noch nicht vollständig geklärt.
Im Rahmen des bereits durchgeführten einstweiligen Rechtsschutzverfahren hat das BVerfG diese Frage noch nicht beantwortet. Vielmehr wurde zum Schutz des Beschwerdeführers angeordnet, dass alle den E-Mail-Account betreffenden Daten vorerst beim AG Braunschweig in Verwahrung zu geben und zu versiegeln sind, aber (noch) nicht verwertet werden dürfen.[85] Die erforderliche Folgenabwägung habe ergeben, dass eine solche Anordnung geboten sei, um erhebliche Nachteile für den Betroffenen für den Fall abzuwenden, dass die verfassungsrechtliche Prüfung ergibt, dass die Datenerhebung auf der Basis der §§ 94, 98 StPO unzulässig war.

Die im Rahmen des einstweiligen Rechtsschutzverfahrens ergangene Entscheidung des BVerfG deutet aufgrund der im Beschluss verwendeten Formulierung „Speicherung von Daten nach Abschluss der Kommunikation" darauf hin, dass es nach Ansicht des BVerfG nicht nur um ein Zwischenspeichern, sondern auch um ein endgültiges Speichern von Daten geht, da der Kommunikationsvorgang als beendet angesehen wird. Andererseits weist das BVerfG aber nicht einfach nur auf seine grundlegende Entscheidung zur Reichweite von Art. 10 GG hin, sondern betont – wie schon ausgeführt –, die Frage, ob

[84] Vgl. Beschluss vom 12.04.2006, 6 Qs 88/06.
[85] Vgl. BVerfG CR 2006, 383 f.

durch den Zugriff auf E-Mails, die auf einem Server gespeichert sind, in Art. 10 GG eingegriffen wird, sei noch nicht abschließend entschieden.

Im anhängigen Hauptsacheverfahren wird nach Auskunft des BVerfG in absehbarer Zukunft wegen der hohen Arbeitsbelastung des Gerichts keine Entscheidung ergehen können. Auch der Verfahrensausgang ist noch völlig offen.

Für die **aktuelle Praxis im Umgang mit zwischengespeicherten Nachrichten** bedeutet der Ausgang der Entscheidung im einstweiligen Rechtsschutzverfahren aber nicht, dass bis zum Ergehen der Hauptsacheentscheidung keine Beschlagnahme von auf einem Server gespeicherten E-Mails auf der Grundlage der §§ 94, 98 StPO mehr zulässig wäre. Je nach Situation kann im konkreten Fall das Strafverfolgungsinteresse das Interesse des Beschuldigten, dass bis zur Entscheidung des BVerfG kein Datenzugriff erfolgt, überwiegen. Dies ist vor allem dann anzunehmen, wenn ein Beweismittelverlust droht. In diesem Fall sollte eine Beschlagnahme erfolgen und das Material vorerst sichergestellt, jedoch zunächst nicht verwertet werden.
Eine **Verwertung der erlangten Erkenntnisse** dürfte aber dann zulässig sein, wenn sie für weitere Ermittlungsschritte unbedingt erforderlich ist. Zwar könnte man bis zur Klärung der Rechtslage durch das BVerfG „sicherheitshalber“ auf § 100a StPO als Ermächtigungsgrundlage zurückgreifen. Doch ist insofern zu bedenken, dass das Erfordernis des Vorliegens einer Katalogtat eine höhere Voraussetzung darstellt, also auf diesem Wege ein Zugriff auf die auf dem Server gespeicherten Daten nur bei einem Verdacht auf eine Katalogtat erfolgen kann.
Es ist möglich, dass das BVerfG im Hauptsacheverfahren zu dem Ergebnis kommt, dass § 100a StPO nicht einschlägig ist und auf der Basis der §§ 94, 98 StPO ein Zugriff auf die Daten auch bei Taten statthaft sein kann, die nicht zu den Katalogtaten des § 100a StPO gehören.

Nach hiesiger Ansicht sind, wie schon oben ausgeführt, die §§ 94, 98 StPO eine ausreichende Ermächtigungsgrundlage für einen Zugriff auf E-Mails. Die rechtliche Situation einer E-Mail im Webaccount eines Providers ist vergleichbar mit der eines Briefes, der in einem Postfach des Adressaten in den Räumen der Deutschen Post AG zur Abholung durch den Empfänger bereitgelegt wurde. Dieser Brief befindet sich ebenfalls nicht mehr auf dem Transportweg und eine Beschlagnahmeanordnung nach §§ 94, 98 StPO würde sich, wenn der Beschluss räumlich das Postfach umfasst, auch auf den Brief selbst erstrecken. Der Brief befindet sich einer solchen Konstellation zwar im räumlichen

Bereich der Deutschen Post AG, diese hat allerdings keine Verfügungsbefugnis mehr über ihn, wenn sie ihn einmal in das Postfach gesteckt hat. Dass die Deutsche Post AG den Brief dem Postfach rein tatsächlich wieder entnehmen könnte, ist in rechtlicher Hinsicht, mit Blick auf die Abgeschlossenheit des Kommunikationsvorganges, unerheblich.

3.3.7. Schlussfolgerungen

Als mögliche Ermächtigungsgrundlagen für verdeckte Zugriffe auf zwischengespeicherte Daten kommen einerseits die TKÜ-Normen, andererseits die Beschlagnahmenormen der StPO in Betracht. In der überwiegenden Zahl der hier untersuchten Fälle wurden allerdings die Vorschriften zur TKÜ als Rechtsgrundlage herangezogen. Die Vielfalt der Befugnisnormen zeigt sich auch darin, dass zum Teil Kombinationsbeschlüsse erlassen wurden, die sich sowohl auf die TKÜ-Normen als auch auf die Beschlagnahmenormen der StPO stützten. Dies zeigt, dass in der Strafverfolgungspraxis eine erhebliche Unsicherheit darüber besteht, welche Ermächtigungsgrundlage einschlägig ist.

Eine Differenzierung zwischen (technisch) end- und zwischengespeichert ist bei der Betrachtung, welche Grundrechte betroffen sind und welche Ermächtigungsgrundlage dementsprechend einschlägig sein könnte, kein taugliches Abgrenzungskriterium. Vielmehr ist nach der bisherigen Rechtsprechung des BVerfG entscheidend, ob sich die Nachricht/Information **im faktischen Machtbereich des Empfängers bzw. Absenders** befindet oder außerhalb.

Die noch ausstehende Entscheidung des BVerfG im o.g. anhängigen Verfahren ist abzuwarten und wird voraussichtlich eine Klärung der rechtlichen Einordnung der vorliegenden Maßnahme bringen.

III. FAZIT

Das Projekt AGNES hat in erheblichem Maß von der Kooperation der beteiligten Dienststellen profitiert. Die große Unterstützung spielt sich insbesondere in der Gesamtzahl der zurückgesandten Fragebögen und den instruktiven Expertengesprächen wider. Dank dieser beachtlichen Resonanz konnten belastbare empirische Daten zu den untersuchten Themenfeldern und umfangreiche Erkenntnisse und daraus gewonnenen Schlussfolgerungen vor allem zu den polizeipraktischen Problemen bei Ermittlungsverfahren mit Bezug zu den untersuchten Themen gewonnen werden. Insbesondere zu den Themenkomplexen 1 und 2 (§§ 100c ff. StPO akustische Wohnraumüberwachung und § 129a Abs. 2 StGB Bildung terroristischer Vereinigungen) erhielt das Projektteam eine Vielzahl von Rückmeldungen, so dass die hier dargestellten Erfahrungen aufgrund der (fast) vollständigen Erhebung besonders aussagekräftig sind.

KI 15 - RETASAST des BKA geht mit diesem Bericht davon aus, dass die hier vorgestellten Erkenntnisse, primär die enthaltenen Handlungsempfehlungen und Musterformulierungen, zur Arbeitserleichterung in der polizeilichen Praxis beitragen und dabei unterstützen, polizeiliche Ermittlungen effektiv und unter Wahrung rechtsstaatlicher Vorgaben zu führen. Zum anderen geht das Projektteam davon aus, dass der in diesem Bericht aufgezeigte gesetzgeberische Handlungsbedarf auf belastbaren Entscheidungsgrundlagen aufgegriffen werden kann. Auch im Rahmen der Aufgabenwahrnehmung der RETASAST als Zentralstelle für die Polizeien des Bundes und der Länder nach § 2 BKAG werden die Erkenntnisse dieses Berichts weitere Verwendung finden, unter anderem in der Bund-Länder-Fallsammlung[86].

Der Bericht basiert auf Erkenntnissen aus der Praxis und ist für die Anwendung in der Praxis ausgelegt. Um laufende Ermittlungsverfahren nicht zu gefährden, wurden alle Verfahren anonymisiert.

[86] Die Bund-Länder-Fallsammlung erscheint halbjährlich und ist in Extrapol zu finden unter Startseite > Bildung & Wissen > Literatur & Information > Infostellen > RETASAST > Bund-Länder-Fallsammlung.

Zusammenfassend lassen sich als Fazit der durchgeführten Analysen folgende inhaltliche Kernaussagen treffen:

- **Themenkomplex akustische Wohnraumüberwachung gemäß §§ 100c ff. StPO**

  Es bestehen bei den Polizeidienststellen erhebliche Probleme, wie die neuen normativen Vorgaben für die Wohnraumüberwachung zu interpretieren sind. Diese Auslegungsprobleme erschweren die Planung und Durchführung von Wohnraumüberwachungen in der Praxis. Schon die Abgrenzung zwischen Maßnahmen innerhalb bzw. außerhalb von Wohnraum ist oftmals problematisch. Dies liegt vor allem darin begründet, dass der Wohnungsbegriff in der Rechtsprechung eine sehr weite Auslegung erfahren hat. Als ungeklärt gilt weiter, ob – und wenn ja, welche – Begleitmaßnahmen von Beschlüssen nach § 100c StPO umfasst sind. Diese Unsicherheiten in Bezug auf die Handhabung der Norm führen dazu, dass von der Durchführung der Maßnahme Abstand genommen wird, obwohl die rechtlichen Voraussetzungen möglicherweise gegeben sind und die Maßnahme auch angemessen wäre.

  Eine Wohnraumüberwachung ist in der Regel nur Erfolg versprechend, wenn sie von einer Videoüberwachung des Außenbereichs der zu überwachenden Räume begleitet wird. Die somit als obligatorisch zu betrachtende Videoüberwachung ist technisch jedoch im Einzelfall oftmals nur unter erheblichen Schwierigkeiten oder gar nicht zu realisieren. Darüber hinaus ist eine Videoüberwachung im Nahbereich der Wohnung i.e.S. (also z.B. im Treppenhaus eines Mehrfamilienhauses) aus rechtlichen Gründen zur Strafverfolgung unzulässig.

  Bei der Durchführung einer Wohnraumüberwachung bereitet das Erkennen einer (drohenden) Kernbereichsverletzung der polizeilichen Praxis erhebliche Probleme. Dies gilt umso mehr, als eine abschließende Definition des Kernbereichs privater Lebensgestaltung bislang nicht gelungen und auch nicht in Sicht ist. Lediglich einige wenige Einzelfallentscheidungen liegen vor, die Selbstgespräche, Gebete und Gespräche über religiöse Themen sowie Gespräche unter Eheleuten betreffen.

  Schwierigkeiten für die polizeiliche Praxis ergeben sich auch bei fremdsprachigen überwachten Gesprächen und dem Einsatz von Sprachmittlern. Dies gilt vor allem, wenn eine Echtzeitüberwachung durchgeführt werden muss (eine Stunde Überwachung bedeutet in der Regel sechs Stunden Auswertung).

Im Urteil des BVerfG vom 27.02.2008 zur Verfassungswidrigkeit von § 5 Abs. 2 Nr. 11 VSG NRW[87] wurde für Zugriffe auf informationstechnische Systeme die Möglichkeit eines zweistufigen Schutzes des Kernbereichs privater Lebensgestaltung eröffnet.
Dies bedeutet, dass zunächst bei der Anordnung einer Maßnahme Kernbereichsschutz zu realisieren ist; ist dies nicht möglich, genügt adäquater Schutz bei der Auswertung. **Eine Übertragung dieses Konzepts auf die Wohnraumüberwachung ist nach Ansicht des Projektteams rechtlich zulässig und deshalb erwägenswert.**

Im Übrigen ist den Dienststellen, die über eine Wohnraumüberwachung als Ermittlungsinstrument im Einzelfall bedarfsabhängig erwägen, in der Regel nur allzu bewusst, dass für eine erfolgreiche Durchführung einer Wohnraumüberwachung ein sehr hoher Personalaufwand erforderlich ist (mindestens zwölf Personen pro Tag). All dies führt dazu, dass in der Praxis gegenwärtig nur sehr zurückhaltend Gebrauch von der akustischen Wohnraumüberwachung gemacht wird.
Zumeist werden derzeit nur kurzzeitige Überwachungen durchgeführt, weil diese deutlich weniger personalintensiv sind als die im Einzelfall jedoch notwendigen längerfristigen Überwachungsmaßnahmen. Bei kurzzeitigen Überwachungen hat es sich in Einzelfällen als hilfreich erwiesen, diese in permanenter Anwesenheit eines Ermittlungsrichters durchzuführen, der ohne zeitlichen Verzug darüber befinden kann, wann eine Überwachung zur Vermeidung von Eingriffen in den Kernbereich persönlicher Lebensgestaltung abgebrochen bzw. unterbrochen wird. Zwar können alternativ auch automatisierte Aufzeichnungen in Betracht gezogen werden, da bei ihnen eine vertretbare Kosten-Nutzen-Relation gewährleistet ist, doch sind automatisierte Aufzeichnungen aufgrund des Erfordernisses einer negativen Kernbereichsprognose in der Regel nur bei Arbeits-, Betriebs- und Geschäftsräumen zulässig.

Der Schlüssel zur Lösung des derzeitigen Konflikts zwischen einerseits dem rechtsstaatlichen Gebot, die Menschen- und Bürgerrechte zu wahren, und andererseits dem legitimen Ziel, bei schweren Straftaten auch durch effektive und praktisch handhabbare Wohnraumüberwachungen Ermittlungen zu führen, könnte nach Einschätzung der befragten Experten in der Einführung des so genannten „Richterbands“ liegen. Der Begriff Richterband bezeichnet eine durchgängige Aufzeichnung der Wohnraumüberwachung, die jedoch nur dem Gericht zur Auswertung zur Verfügung steht. Das Richterband würde auch dabei helfen, Manipulationen durch Tatverdächtige im Wege

[87] BVerfG NJW 2008, 822 ff.

vorgetäuschter Kernbereichsrelevanz aufzudecken. Es würde aber auch der Wahrung der Interessen von Beschuldigten dienen, da so sichergestellt werden könnte, dass nicht bestimmte entlastende Äußerungen dem Gericht vorenthalten werden.

Insgesamt haben die Untersuchungen zur polizeilichen Praxis der Wohnraumüberwachung ergeben, dass die polizeilichen Dienststellen mit dem Ermittlungsinstrument der Wohnraumüberwachung nach § 100c StPO verantwortungsvoll umgehen.

Gesetzgeberischer Handlungsbedarf wird in folgenden Bereichen für erforderlich erachtet:

- Einführung des Richterbandes,
- zweistufiger Kernbereichsschutz zumindest bei fremdsprachigen Gesprächen,
- Relativierung des Gebots des unverzüglichen Löschens von Aufzeichnungen,
- Videoüberwachung im Nahbereich von Wohnungen (z.B. im Hausflur großer Gebäudekomplexe),
- ggf. Mitwirkung Dritter im Rahmen von Begleitmaßnahmen.

- **Themenkomplex Bildung terroristischer Vereinigungen gemäß § 129a Abs. 2 StGB**

  Entgegen der Erwartung, die zu Beginn des Projekts bestand, lagen die Probleme bei der Anwendung des § 129a Abs. 2 StGB nicht im subjektiven Tatbestand, hier vor allen Dingen dem Nachweis der terroristischen Absicht, sondern aufgrund der aktuellen Rechtsprechung des BGH im objektiven Tatbestand, und zwar bei der Frage der Eignung der Tat zur Schädigung der Schutzgüter der Norm.
  Die im Rahmen des Projekts durchgeführten Verfahrensevaluationen und die Hintergrundgespräche haben ergeben, dass ein Reformbedarf bezüglich § 129a Abs. 2 StGB aus polizeipraktischer Sicht derzeit nicht gegeben ist.
  Zwar wurde eine hohe Strafbarkeitshürde errichtet, indem als Teil des objektiven Tatbestands normiert wurde, dass die Tat zur ernsthaften Schädigung der Schutzgüter des Tatbestands – etwa der Grundstrukturen eines Staates oder einer internationalen Organisation – geeignet sein muss. Insoweit ist aber zu berücksichtigen, dass die Anforderungen an die Eignung der Tat zur ernsthaften Schädigung zu Beginn eines Verfahrens nicht zu hoch angesetzt werden dürfen. Ob tatsächlich eine solche Eignung gegeben ist, kann erst im Zuge der durchzuführenden Ermittlungen verbindlich beantwortet werden. Dies bedeutet aber zugleich, dass während eines laufenden

Ermittlungsverfahrens permanent aufgrund der neu gewonnenen Erkenntnisse überprüft werden muss, ob tatsächlich hinreichende Anhaltspunkte für das Vorliegen einer Schädigungseignung der Tat gegeben sind.
Die Rechtsprechung des BGH zu § 129a Abs. 2 StGB zeigt deutlich, dass eine Einzelfallbetrachtung erforderlich ist: Brandstiftungen an Gewerbebetrieben ausländischer Mitbürger mit der Intention, einen Teil Deutschlands „ausländerfrei zu machen“, erfüllen den Tatbestand, Brandstiftungen an Gebäuden und Sachen mit durchaus hohem Sachschaden, die einen Umsturz des politischen Systems bewirken sollen, hierzu aber nicht geeignet sind, dagegen nicht.

- **Themenkomplex Ermittlungspraxis im Zusammenhang mit der Nutzung moderner Kommunikationsmittel**

  In der polizeilichen Praxis wird der Bedarf an der Normierung einer **repressiven Online-Durchsuchung** eindeutig bejaht. Es besteht insofern Einigkeit, dass die repressive Online-Durchsuchung keine weitere „Standardmaßnahme“ darstellt, sondern lediglich zur Bekämpfung schwerster Kriminalität und unter strengen Voraussetzungen eingesetzt werden wird. Insbesondere die stetig zunehmende Kryptierung der Daten auf einem PC im Bereich der Schwerkriminalität gebietet nach Ansicht der polizeilichen Praxis, die Online-Durchsuchung in einem engen rechtsstaatlichen Rahmen zuzulassen.

  Unter Beachtung verfassungsrechtlicher Vorgaben wie einem

  - grundsätzlichen Richtervorbehalt,
  - zweistufigen Kernbereichsschutz mit Löschungsvorschriften sowie Verwertungsverboten

  ist die Normierung einer Online-Durchsuchung zum Schutz herausragender Rechtsgüter sowohl zu Zwecken der Gefahrenabwehr wie auch zur Strafverfolgung zulässig. Ein Recht zum Betreten von Wohnraum zur Installation der Software wäre als wichtige Einbringungsmöglichkeit dargestellt.

  Eine **Quellen-TKÜ** – hierunter versteht man den Zugriff auf laufende, verschlüsselte Kommunikation am Ort der Datenversendung bzw. des Datenempfangs[88] – ist, wurde bislang auf § 100a StPO gestützt. Ob die Gerichte nach der Entscheidung des Bundesverfassungsgerichts zur Online-Durchsuchung bei dieser Praxis bleiben, bleibt abzuwarten..

Für einen **Zugriff auf zwischengespeicherte Daten** werden in der polizeilichen und justiziellen Praxis derzeit verschiedene Ermächtigungsgrundlagen der StPO (Beschlagnahme, TKÜ sowie eine Kombination der beiden) herangezogen. Eine klare, durch höchstrichterliche Rechtsprechung bestätigte Linie hat sich bislang nicht entwickelt. Es ist mithin noch nicht endgültig geklärt, welche Befugnisnorm für solche Maßnahmen die „richtige" ist bzw. ob gleich mehrere Normen der StPO derartige Maßnahmen gestatten. Allerdings ist eine gewisse Tendenz dahingehend auszumachen, Rückgriff auf § 100a StPO zu nehmen.

Eindeutig ist die Tendenz zum Rückgriff auf § 100a StPO hinsichtlich der verdeckten **Teilnahme an geschlossenen Chats** erkennbar. Beim verdeckten Zugriff auf zwischengespeicherte Daten wurde zumindest die überwiegende Anzahl der Maßnahmen auf § 100a StPO gestützt. § 100a StPO ist daher – jedenfalls derzeit – für die Polizeipraxis die zentrale Ermächtigungsgrundlage gleichermaßen für Zugriffe auf Daten im Rahmen einer Chatteilnahme wie bei zwischengespeicherten Daten.

Die festgestellte Tendenz, polizeiliche Maßnahmen auf § 100a StPO zu stützen, da diese Norm im Vergleich zu anderen Ermächtigungsgrundlagen die höchsten Eingriffsvoraussetzungen aufstellt und damit eine vermeintlich sichere rechtliche Basis darstellt, ist nicht nur methodisch unzulässig, da unabhängig von den aufgestellten rechtlichen Hürden zu prüfen ist, ob eine Norm den beabsichtigten Eingriff erfasst oder nicht. Ein solches Vorgehen ist auch deshalb bedenklich, weil damit polizeiliche Eingriffe unter Umständen ohne rechtliche Notwendigkeit unterbleiben, nur weil die hohen Eingriffsvoraussetzungen des § 100a StPO nicht erfüllt sind.

Auf zwischengespeicherte Nachrichten kann beispielsweise nach hiesiger Ansicht bereits aufgrund der – recht weit gefassten – Beschlagnahmenormen der §§ 94, 98 StPO zugegriffen werden. Dies gilt gleichermaßen bei offenen als auch bei verdeckten Zugriffen. Bei letzteren allerdings nur, wenn offene Maßnahmen vorangegangen sind und aufgrund dieser Erkenntnisse ein Zugriff ermöglicht wird.

Von dem Ermittlungsinstrument der polizeilichen Chatteilnahme wird in der Praxis sehr selten Gebrauch gemacht. Dies liegt daran, dass eine DSL-Ausleitung der stattfindenden Kommunikation einfacher realisierbar ist als eine Chatteilnahme und kein Entdeckungsrisiko für die Polizei besteht. Allerdings scheitert eine DSL-Ausleitung immer dann,

[88] Vgl. hierzu BVerfG NJW 2008, 822 (825, Rz. 184, 188 ff.).

wenn im Chat kryptiert kommuniziert wird. Sofern dies der Fall ist, ist eine Teilnahme am geschlossenen Chat unabdingbar; die Teilnahme stellt dann laut BVerfG einen Eingriff in Art. 10 GG dar[89] und kann folglich auf § 100a StPO gestützt werden.

[89] BVerfG NJW 2008, 822 (835, Rz. 292).

IV. ANHANG

1. Literaturempfehlung

1.1. Beiträge zur Wohnraumüberwachung

1.1.1. Aufsätze zur repressiven akustischen Wohnraumüberwachung

- *Büddefeld*, *Dieter*

  Akustische Wohnraumüberwachung, Kriminalistik 2005, 204 ff.

- *Kutscha*, *Martin*
  Verfassungsrechtlicher Schutz des Kernbereichs privater Lebensgestaltung – nichts Neues aus Karlsruhe?, NJW 2005, 20 ff.

- *Leutheusser-Schnarrenberger*, *Sabine*
  Der Gesetzentwurf der Bundesregierung zum „Großen Lauschangriff“, ZRP 2005, 1 ff.

- *Löffelmann*, *Markus*
  Die Neuregelung der akustischen Wohnraumüberwachung, NJW 2005, 2033 ff.

- *Nack*, *Armin*
  Akustische Wohnraumüberwachung und Verwertungsverbot, in Festschrift für Kay Nehm zum 65. Geburtstag, 2006, S. 310 ff.

- *Rauschenberger*, *Friederike*
  Heimliches Abhören und Aufzeichnen des nichtöffentlich gesprochenen Wortes innerhalb von Wohnungen, Kriminalistik 2005, 654 ff.

1.1.2. Aufsätze zur Verwertbarkeit eines Selbstgesprächs

- *Ellbogen*, *Klaus*
  Anmerkung, NStZ 2006, 180 f

- *Kolz*, *Michael*
  Das Selbstgespräch im Krankenzimmer und der „Große Lauschangriff“, NJW 2005, 3248 ff.

- *Lindemann*, *Brian*
  Der Schutz des „Kernbereichs privater Lebensgestaltung“ im Strafverfahren, JR 2006, 191 ff.

- *Valerius*,
  Grenzen des Großen Lauschangriffs, JA 2006, 15 f.

1.1.3. Aufsatz zur präventiven akustischen Wohnraumüberwachung

- *Perne*, *Volker*
  Richterband und Kernbereichsschutz – Zur verfassungsrechtlichen Problematik des nachträglichen Lauschens und Spähens durch den Richter, DVBl. 2006, 1486 ff.

1.1.4. Dissertation zum Kernbereichsschutz

- *Warntjen*, *Maximilian*
  Heimliche Zwangsmaßnahmen und der Kernbereich privater Lebensgestaltung, Baden-Baden 2007

1.2. Beiträge zur Bildung terroristischer Vereinigungen

1.2.1. Aufsätze zu § 129a StGB

- *Helm*, *Martin*
  Die Bildung terroristischer Vereinigungen – Auslegungsprobleme beim neuen § 129a StGB, StV 2006, 719 ff.

- *Weigend*, *Thomas*
  Terrorismus als Rechtsproblem, Festschrift für Kay Nehm zum 65. Geburtstag, 2006, S. 151 ff.

1.2.2. Aufsätze zu § 129b StGB:

- *Altvater*, *Gerhard*
  Das 34. Strafrechtsänderungsgesetz - § 129 b StGB, NStZ 2003, 179 ff.

- *Betmann*, *Christian*
  § 129b StGB – sinnvolles besonderes Strafanwendungsrecht, Kriminalistik 2006, 186 ff.

- *Rauschenberger*, *Friederike*
  Bildung krimineller Vereinigungen, Kriminalistik 2001, 772 ff.

- *Stein*, *Ulrich*
  Kriminelle und terroristische Vereinigungen mit Auslandsbezug seit der Einführung von § 129b StGB, GA 2005, 433 ff.

1.2.3. Aufsatz zum Vereinigungsbegriff

- *Von Heintschel-Heinegg*, *Bernd*
  Gemeinschaftsrechtskonforme Auslegung des Vereinigungsbegriffs in den §§ 129 ff. StGB, Festschrift Schroeder, 2006, S. 799 ff.

1.3. Zum Themenkomplex Ermittlungspraxis mit der Nutzung moderner Kommunikationsmittel

1.3.1. Beiträge zur Online-Durchsuchung

- *Buermeyer*, *Ulf*
  Die „Online-Durchsuchung". Verfassungsrechtliche Grenzen des verdeckten hoheitlichen Zugriffs auf Computersysteme, HRRS 2007, 329 ff.

- *Gercke*, *Marco*
  Heimliche Online-Durchsuchung: Anspruch und Wirklichkeit, CR 2007, 245 ff.

- *Hornung*, *Gerrit*
  Ermächtigungsgrundlage für die „Online-Durchsuchung", DuD 2007, 575 ff.

- *Jahn, Matthias/Kudlich*, *Hans*
  Die strafprozessuale Zulässigkeit der Online-Durchsuchung, JR 2007, 57 ff.

- *Kemper, Martin*
  Anforderungen und Inhalt der Online-Durchsuchung bei der Verfolgung von Straftaten, ZRP 2007, 105 ff.

- *Kutscha*, *Martin*
  Verdeckte „Online-Durchsuchung" und Verletzlichkeit der Wohnung, NJW 2007, 1169 ff.

- *Rux*, *Johannes*
  Ausforschung privater Rechner durch die Polizei- und Sicherheitsbehörden, JZ 2007, 285 ff.

- *Schlegel*, *Stephan*
  Warum die Festplatte keine Wohnung ist – Art. 13 GG und die Online-Durchsuchung", GA 2007, 648 ff.

1.3.2. Aufsatz zu § 5 VerfSG NRW

- *Huber*, *Bertold*
  Trojaner mit Schlapphut – heimliche „Online-Durchsuchung" nach dem Nordrhein-Westfälischen Verfassungsschutzgesetz, NVwZ 2007, 880 ff.

1.3.3. Anmerkungen zu BGH, Beschluss vom 31.01.2007

- *Bär*, *Wolfgang*; MMR 2007, 239 ff.
- *Cornelius*, *Kai*; JZ 2007, 798 ff.
- *Fezer*, *Gerhard*; NStZ 2007, 535 f.
- *Harrendorf*, *Stefan* ; StraFo2007, 149 ff.
- *Hornung*, *Gerrit* ; CR 2007, 144 f.
- *Schaar, Peter/Landwehr*, *Sebastian*; K&R 2007, 202 ff.

1.3.4. Aufsatz zur Quellen-TKÜ

- *Sankol*, *Barry*
  Überwachung von Internet-Telefonie, CR 2008, 13 ff.

1.3.5. Beiträge zum verdeckten Zugriff auf zwischengespeicherte Nachrichten

- *Jahn*, *Matthias*
  Der strafprozessuale Zugriff auf Telekommunikationsverbindungsdaten – BVerfG, NJW 2006, 976, JuS 2006, S. 491 ff.

- *Keller*, *Christoph*
  Online-Durchsuchung und Überwachung des E-Mail-Verkehrs, DPolBl 2007, S. 24 ff.

1.3.6. Dissertation zum Zugriff auf E-Mail-Kommunikation

- *Störing*, *Marc*
  Strafprozessuale Zugriffsmöglichkeiten auf E-Mail-Kommunikation, Berlin 2007

1.3.7. Anmerkungen zur Entscheidung des BVerfG zum offenen Zugriff auf zwischengespeicherte E-Mails im einstweiligen Rechtsschutz

- *Sankol*, *Barry*
  MMR 2007, S. 170 f.

- *Schlegel*, *Stephan*
  „Beschlagnahme“ von E-Mail-Verkehr beim Provider, HRRS 2007, S. 44 ff.

2. Erhebungsbögen

2.1. §§ 100c ff. StPO, akustische Wohnraumüberwachung

Bitte **pro WRÜ-Maßnahme** einen Bogen ausfüllen.
Die Erhebung bezieht sich auf den Zeitraum ab März 2004.

Dienststelle:
telefonische Erreichbarkeit:

I. Anordnung nach §§ 100c ff. StPO	
1. Warum wurde die WRÜ-Maßnahme im Ermittlungsverfahren für erfolgversprechend gehalten *[ggf. mehrere Gründe eintragen]*?	
2. Welche Katalogtat(en) waren Anlass für das Ermittlungsverfahren *[hier bitte die Norm(en) nennen]*?	
3. Für welchen Zeitraum (ggf. gerundet) wurde die Überwachung **a)** erstmals angeordnet **b)** in der Verlängerung angeordnet?	a) Wochen b) Wochen
4. Wie lange dauerte die Überwachung tatsächlich **a)** in der erstmaligen Anordnung? **b)** in der Verlängerung?	a) Wochen b) Wochen
5. Bezog sich die WRÜ-Maßnahme *[Mehrfachnennungen möglich]*	auf Privatwohnungen auf ABG-Räume (Geschäftsräume, Publikumsverkehr, …) auf sonstige geschützte Räume (Krankenzimmer o.ä.)
6. Bitte benennen Sie die Räumlichkeit(en) konkret:	

II. Abgelehnte und nicht durchgeführte Maßnahmen	
1. Wurde der Antrag auf Erlass eines WRÜ-Beschlusses abgelehnt?	Nein (weiter zu 2.) Ja, und zwar auf Grund polizeilicher Erwägungen Ja, und zwar durch die Staatsanwaltschaft Ja, und zwar durch das Gericht
Wenn ja, mit welcher Begründung *[ggf. mehrere Gründe eintragen]*?	
2. Wurde auf die Durchführung der WRÜ-Maßnahme trotz Vorliegens einer Anordnung verzichtet?	Nein (weiter zu 3.) Ja
Wenn ja, warum *[ggf. mehrere Gründe eintragen]*?	
3. Wurde auf die Durchführung einer WRÜ-Maßnahme verzichtet oder diese unterbrochen, weil Berufsgeheimnisträger betroffen waren?	Nein Ja
Wenn ja, um welche Art Berufsgeheimnisträger handelte es sich?	
III. Vorbereitung	
1. Wie viele Tage dauerte die Vorbereitung der technischen Umsetzung der WRÜ nach der Anordnung?	Tage
2. Welche flankierenden Maßnahmen waren erforderlich, um eine WRÜ technisch durchführen zu können (z.B. Öffnen von gesicherten Türen, Betreten der Wohnung, Observation etc.) *[bitte alle benennen]*?	
IV. Durchführung	
1. Wurde ein Live-Mithören angeordnet?	Nein (weiter zu IV b.) Ja (weiter zu 1.1)
1.1 Durch wen?	Durch den Ermittlungsführer Durch die Staatsanwaltschaft Durch das Gericht
1.2 Das Live-Mithören war	dauerhaft angeordnet zeitweise angeordnet
2. Welche Probleme ergaben sich beim Live-Mithören von nichtöffentlichen Gesprächen?	

IV a. Schutz des Kernbereichs privater Lebensgestaltung	
1. Musste eine Live-Abhörmaßnahme aus Kernbereichsschutzgründen unterbrochen bzw. abgebrochen werden?	Nein (weiter zu 4.) Ja (weiter zu 1.1)
1.1 Wie oft wurde die Maßnahme unterbrochen?	
1.2 Aufgrund welcher Informationen wurde eine Kernbereichsbetroffenheit angenommen?	
1.3 Wer hat über die Unterbrechung bzw. den Abbruch entschieden?	der Ermittlungsführer die Staatsanwaltschaft das Gericht
2. Nach wie vielen Stunden wurde nach einer Unterbrechung durchschnittlich wieder zugeschaltet?	Stunden
2.1 Warum wurde die Unterbrechung wieder aufgehoben?	
2.2 Wer hat darüber entschieden?	der Ermittlungsführer die Staatsanwaltschaft das Gericht
3. Ergaben sich durch die Unterbrechung Probleme für die Beweisverwertbarkeit?	Unbekannt – das Verfahren ist noch nicht abgeschlossen Nein Ja, und zwar
4. Erfolgte die Klärung des Kernbereichs durch Vorlage bei Gericht (§ 100c VII StPO)?	Nein (weiter zu IV b.) Ja
Wenn ja, deckte sich die Entscheidung des Gerichts mit der eigenen Einschätzung?	Nein Ja
IV b. Begleitmaßnahmen	
1. Waren begleitende Maßnahmen erforderlich, um die Wohnraumüberwachung aufrecht zu erhalten?	Nein (weiter zu 2.) Ja
Wenn ja, welche *[bitte alle benennen]*?	
2. Welche begleitenden Maßnahmen waren erforderlich, um nach Beendigung der WRÜ in den Räumlichkeiten befindliche technische Geräte zu entfernen *[bitte alle benennen]*?	

3. Wurden weitere Ermittlungsmaßnahmen durchgeführt, um das Wiederzuschalten nach einer Unterbrechung zu ermöglichen?	Nein (weiter zu 4.) Ja
Wenn ja, welche *[bitte alle benennen]*?	
4. Wurden optische Maßnahmen durchgeführt, um die Gespräche bestimmten Personen zuordnen zu können?	Nein (weiter zu 5.) Ja
Wenn ja, welche *[bitte alle benennen]*?	
5. Wurden bei der Durchführung einer WRÜ vor der gesetzlichen Neuregelung (März 2004 bis Juli 2005) Maßnahmen zum Schutz des Kernbereichs ergriffen?	Nein (weiter zu 6.) Ja
Wenn ja, welche *[bitte alle benennen]*?	
6. Wurden Techniker eingesetzt?	Nein Ja
7. Wurden Sprachmittler eingesetzt?	Nein Ja
V. Angaben zu den Betroffenen	
1. Wer war Inhaber der betroffenen Räume?	die beschuldigte Person (ein) Dritte(r), nämlich
2. Wie viele unbeteiligte Dritte (Anzahl) waren durch die WRÜ-Maßnahme a) in erheblichen Maß betroffen? b) in nicht erheblichen Maß betroffen?	a) Personen b) Personen
3. Wie viele zeugnisverweigerungsberechtigte Personen waren durch die Maßnahme betroffen?	Personen
4. Lag ein Einverständnis des Wohnungsinhabers mit der Überwachung vor?	Nein Ja

VI. Nachbereitung	
1. Wurden WRÜ-Maßnahmen wegen Wegfalls der Voraussetzungen vor Ablauf der Frist beendet?	Nein (weiter zu 2.) Ja (weiter zu 1.1)
1.1 Welche Ursachen lagen der Beendigung zu Grunde *[Mehrfachnennungen möglich]*?	taktische rechtliche technische
1.2 Wie lange vor Ablauf der Frist wurde die Maßnahme beendet?	Tage vor Ablauf
2. Wurden von der WRÜ-Maßnahme betroffene Personen von der Durchführung der Maßnahme benachrichtigt *[soweit bekannt]*?	Nein (weiter zu 3.) Ja Bisher nicht (weiter zu 2.1)
2.1 Wie lange wurde die Benachrichtigung zurückgestellt (ggf. gerundet) *[soweit bekannt]*?	Wochen
2.2 Warum wurde die Benachrichtigung zurückgestellt *[soweit bekannt]*?	
3. Wie viele von der Maßnahme erheblich Betroffene wurden von der Durchführung der Maßnahme abschließend nicht benachrichtigt *[soweit bekannt]*?	
VII. Ergebnis der Wohnraumüberwachung	
1. Die WRÜ-Maßnahme führte *[Mehrfachnennungen möglich]*	zur Ermittlung des Aufenthalts des Beschuldigten zur Ermittlung des Aufenthalts anderer Gesuchter zur Aufklärung des Sachverhalts zu keinem Ergebnis
2. Die Maßnahme führte zu Erkenntnissen, die **...** Relevanz für **...** hatten. *[Mehrfachnennungen möglich]*	unmittelbare – das Anlassverfahren (weiter zu 4.) mittelbare – das Anlassverfahren unmittelbare – andere Verfahren mittelbare – andere Verfahren nicht verfahrensrelevant waren
3. Waren die Straftaten, für deren Ermittlungen die Zufallsfunde Relevanz hatten, Katalogstraftaten des § 100c StPO?	Nein Ja, und zwar

4. Wurden Erkenntnisse aus der WRÜ zu Zwecken der Gefahrenabwehr verwendet?	Nein Ja
VIII. Allgemeine Angaben	
1. Ging der Erwägung, eine WRÜ-Maßnahme nach §§ 100c ff. StPO durchzuführen, eine auf präventive Normen gestützte WRÜ voraus?	Nein (weiter zu 3.) Ja
1.1 Wenn ja, auf welche Norm(en) wurde die (präventive) WRÜ gestützt?	
1.2 Ergaben sich hierbei Probleme (z.B. Schutz des Kernbereichs)?	Nein Ja, und zwar
2. Wurden Erkenntnisse aus der präventiven WRÜ in das Strafverfahren eingebracht?	Nein Ja
3. Wurden WRÜ-Maßnahmen zur Eigensicherung durchgeführt?	Nein Ja
3.1 Aufgrund welcher Rechtsgrundlage?	
3.2. Ergaben sich hierbei Probleme (z.B. Schutz des Kernbereichs)?	Nein Ja, und zwar

Vielen Dank!

2.2. § 129a Abs. 2 StGB, Bildung terroristischer Vereinigungen

Bitte pro Verfahren, in dem ein Ermittlungsverfahren nach § 129a Abs. 2 StGB durchgeführt wurde oder auch nur angedacht war, jeweils einen Bogen ausfüllen.

Die Erhebung bezieht sich auf den Zeitraum ab 2004.
Der Gesetzestext des § 129a StGB ist im Anhang abgedruckt.

Dienststelle:

telefonische Erreichbarkeit:

I. Probleme bei der Begründung des Anfangsverdachtes nach § 129a Abs. 2 StGB	
1. Wurde das Verfahren wegen des Verdachts auf Gründung einer terroristischen Vereinigung nach § 129a Abs. 2 StGB eingeleitet?	Nein (weiter zu 2.) Ja (weiter zu II.)
2. Fehlten Anhaltspunkte für den Verdacht der terroristischen Vereinigung hinsichtlich des **objektiven Tatbestandes**?	Nein Ja
a) Wenn ja, warum?	
b) Das Verfahren wurde aber statt dessen geführt wegen des Verdachts nach *[bitte Norm(en) benennen]*:	
3. Fehlten Anhaltspunkte für den Verdacht der terroristischen Vereinigung hinsichtlich des **subjektiven Tatbestandes**?	Nein Ja
a) Wenn ja, warum?	
b) Das Verfahren wurde aber statt dessen geführt wegen des Verdachts nach *[bitte Norm(en) benennen]*:	
II. Katalogtaten des § 129a Abs. 2 StGB	
1. Der **Gründung** der Vereinigung lag zu Grunde, dass sich der Zweck oder die Tätigkeit darauf richtete, *a) einem anderen Menschen schwere körperliche oder seelische Schäden, insbesondere der in § 226 StGB bezeichneten Art, zuzufügen,* *b) Straftaten nach den §§ 303b, 305, 305a StGB oder gemeingefährliche Straftaten in bestimmten*	Der Tatbestand der Gründung war nicht erfüllt. a) in diesem Fall b) in diesem Fall c) in diesem Fall d) in diesem Fall e) in diesem Fall

Fällen *c) Straftaten gegen die Umwelt in den Fällen des § 330a Abs. 1 bis 3,* *d) Straftaten nach bestimmten Normen des Gesetzes über die Kontrolle von Kriegswaffen oder* *e) Straftaten nach § 51 Abs. 1 bis 3 des Waffengesetzes* zu begehen [hier bitte die Katalogtat(en) benennen]:	
2. Der **Beteiligung** als Mitglied an der Vereinigung lag zu Grunde, dass sich der Zweck oder die Tätigkeit darauf richtete, eine unter 1. genannte Katalogtat zu begehen *[hier bitte die Katalogtat(en) benennen]*:	Der Tatbestand der Beteiligung war nicht erfüllt. a) in diesem Fall b) in diesem Fall c) in diesem Fall d) in diesem Fall e) in diesem Fall
III. Sonstiger objektiver Tatbestand des § 129a Abs. 2 StGB	
1. Wie hat sich der Beschuldigte an der Gründung der Vereinigung beteiligt?	
2. Wie hat sich der Beschuldigte als Mitglied der Vereinigung beteiligt?	
3. Auf welche Dauer ist/war die Vereinigung angelegt (Erkenntnisstand bei Begründung des Anfangsverdachts und - falls abweichend - im weiteren Verfahren)?	
4. Wie viele Mitglieder hat/hatte die Vereinigung **a)** dem Verdacht nach zu Beginn der Ermittlungen? **b)** dem Verdacht nach während des weiteren Ermittlungsverfahrens? **c)** am Ende nachweislich?	a) b) c)
5. Anhand welcher Kriterien wurde bei Begründung des Anfangsverdachtes und im Laufe des Ermittlungsverfahrens die Eignung der Tat, einen Staat oder eine internationale Organisation	

a) durch die Art der Begehung der unter II. genannten Katalogtat oder **b)** ihrer Auswirkungen ernsthaft zu schädigen, begründet?	a) b)
IV. Subjektiver Tatbestand des § 129a Abs. 2 StGB	
1. Die **Tat** nach § 129a Abs. 2 StGB **muss dazu bestimmt sein**, die Bevölkerung auf erhebliche Weise **einzuschüchtern**, eine Behörde oder eine internationale Organisation rechtswidrig mit Gewalt oder durch Drohung mit Gewalt **zu nötigen** oder die politischen, verfassungsrechtlichen, wirtschaftlichen oder sozialen Grundstrukturen eines Staates oder einer internationalen Organisation zu beseitigen oder **erheblich zu beeinträchtigen (terroristische Absicht)**.	
a) Wodurch/in welcher Variante wurde insoweit der Anfangsverdacht begründet?	a)
b) Wodurch wurden insoweit während des Ermittlungsverfahrens richterliche Anordnungen begründet?	b)
c) Soweit bekannt: Wodurch wurde insoweit die Anklageschrift begründet?	c)
d) Soweit bekannt: Wodurch wurde insoweit das Urteil begründet?	d)
e) Welche Probleme ergaben sich bei a)-d)?	e)
f) Hat sich die o.g. Zweckrichtung (Bestimmung) der Vereinigung auch realisiert? Wenn ja, wie?	f) Nein Ja, und zwar durch …

2. Durch die Art der Begehung der Tat oder ihrer Auswirkungen muss **ein Staat oder eine internationale Organisation erheblich geschädigt werden können**. **a)** Wodurch wurde insoweit der Anfangsverdacht begründet? **b)** Wodurch wurden insoweit während des Ermittlungsverfahrens richterliche Anordnungen begründet? **c)** Soweit bekannt: Wodurch wurde insoweit die Anklageschrift begründet? **d)** Soweit bekannt: Wodurch wurde insoweit das Urteil begründet? **e)** Welche Probleme ergaben sich bei a)-d)?	a) b) c) d) e)
3. Mit welchen Ermittlungshandlungen konnte der subjektive Tatbestand belegt werden *[Mehrfachnennungen möglich]*?	Vernehmung Sachbeweis Verdeckte Maßnahmen (z.B. TKÜ, VE, VP) Ermittlungshandlung(en) bitte jeweils konkret benennen:
4. Wenn TKÜ-Erkenntnisse vorlagen, wurden diese unmittelbar in das Beweisverfahren eingebracht?	Nein Ja

Vielen Dank!

2.3. Online-Durchsuchung

Eine Online-Durchsuchung im Sinne dieses Erhebungsbogens ist beschränkt auf Fallkonstellationen, in denen durch den Einsatz spezieller elektronischer Mittel (Trojanischer Pferde oder sonstiger Software) ein heimlicher Zugriff auf (typischerweise auf einem Endgerät) gespeicherte Daten ermöglicht wird. Hierdurch soll die Kenntnisnahme des Inhaltes der Daten durch die Polizei erreicht werden, z.B. durch eine unbemerkt über die Software veranlasste Übermittlung der Daten.

Keine Online-Durchsuchung in diesem Sinne ist

- der offene Zugriff auf Daten
- der Einsatz von Hardware
- der (verdeckte) Zugriff auf Daten unter Benutzung eines durch andere Maßnahmen erlangten Passwortes
- die Teilnahme an einem geschlossenen Chat
- die sog. Quellen-TKÜ, auch aktive TKÜ genannt, d.h. die Überwachung von Telekommunikationsinhalten ohne Inanspruchnahme des Netzbetreibers

Seit dem Beschluss des BGH vom 31.01.2007 sind repressive verdeckte Online-Durchsuchungen als unzulässig zu erachten, da in der StPO keine Rechtsgrundlage vorhanden ist. Es besteht daher Bedarf an der Schaffung einer Befugnis für Online-Durchsuchungen. Dieser Bedarf kann nur mithilfe einer hohen Anzahl an Rechtstatsachen glaubhaft belegt werden.

Bitte pro repressiver oder präventiver Online-Durchsuchung, die durchgeführt wurde oder auch nur angedacht war, einen Bogen ausfüllen.

Dienststelle:

telefonische Erreichbarkeit:

I. Allgemeine Informationen	
4. Welche Anhaltspunkte lagen vor, dass eine Online-Durchsuchung für das Verfahren bzw. die Abwehr einer Gefahr förderlich sein könnte [bitte alle benennen]?	
5. Die Online-Durchsuchung wurde	nur angedacht – II./VII. ausfüllen beantragt, aber abgelehnt - III./VII. ausfüllen genehmigt, aber nicht durchgeführt (IV./VII.) durchgeführt (weiter bei V.)

II. Angedachte Online-Durchsuchung	
1. Welche Maßnahmen gingen der angedachten Online-Durchsuchung **voraus** [bitte alle benennen]?	
2. Auf welche Rechtsgrundlage(n) sollte die Online-Durchsuchung gestützt werden?	
3. Mit welcher Begründung wurde von einer Online-Durchsuchung abgesehen?	aufgrund des BGH-Beschlusses vom 31.1.07 aufgrund von anderen Gründen, und zwar…
III. Beantragter, aber abgelehnter Beschluss zur Online-Durchsuchung	
3. Welche Maßnahmen gingen der beantragten Online-Durchsuchung **voraus** [bitte alle benennen]?	
4. Auf welche Rechtsgrundlage(n) wurde der Antrag gestützt?	
5. Mit welcher Begründung wurde der Antrag abgelehnt?	aufgrund des BGH-Beschlusses vom 31.1.07 aufgrund von anderen Gründen, und zwar…
IV. Nicht realisierter Beschluss zur Online-Durchsuchung	
1. Welche Maßnahmen gingen der beantragten Online-Durchsuchung **voraus** [bitte alle benennen]?	
2. Auf welche Rechtsgrundlage(n) wurde der **Antrag** zur Online-Durchsuchung gestützt?	
3. Auf welche Rechtsgrundlage(n) wurde der **Beschluss** zur Online-Durchsuchung gestützt?	
4. Wie lautete die Begründung des Beschlusses?	
5. Warum wurde die Online-Durchsuchung nicht durchgeführt?	
V. Durchgeführte Online-Durchsuchung	
6. Welche Maßnahmen gingen dem Beschluss zur Online-Durchsuchung **voraus** [bitte alle	

benennen]?	
7. Auf welche Rechtsgrundlage(n) wurde der **Antrag** zur Online-Durchsuchung gestützt?	
8. Auf welche Rechtsgrundlage(n) wurde der **Beschluss** zur Online-Durchsuchung gestützt?	
9. Wie lautete die Begründung des Beschlusses?	
10. Die Online-Durchsuchung war	zum einmaligen Zugriff auf Daten angelegt als längerfristige Maßnahme ausgelegt
Wenn längerfristig, wie lange?	Tage
11. Welche Maßnahmen erfolgten **im Anschluss** an die Online-Durchsuchung [bitte alle benennen]?	
12. War bei der Online-Durchsuchung eine Mitwirkung des Tatverdächtigen erforderlich (z.B. Öffnen eines E-Mail-Anhangs)?	Ja Nein
Wenn ja, welcher Art?	
13. Ergaben sich sonstige Probleme bei der Durchführung der Online-Durchsuchung?	
VI. Erfolg der Online-Durchsuchung	
1. Hatte die Online-Durchsuchung einen Mehrwert für [Mehrfachnennungen möglich]	... das Anlassverfahren bzw. die Abwehr einer Gefahr? Ja Nein ... andere Ermittlungsverfahren (Zufallsfunde)? Ja Nein
2. Wurden die durch die Online-Durchsuchung gewonnenen Erkenntnisse als Beweismittel in ein Gerichtsverfahren eingebracht?	Ja Nein

Wenn ja, wie (z.B. Protokollverlesung, Zeugenbeweis)?	
VII. Genereller Bedarf an einer Regelung zur Online-Durchsuchung	
1. In welchen Fällen sehen Sie Bedarf für eine (verdeckte) Online-Durchsuchung zu Strafverfolgungszwecken?	
2. Wären die Erkenntnisse, die durch eine Online-Durchsuchung hätten gewonnen werden können, auch mittels anderer Maßnahmen zu erlangen gewesen?	Ja Nein
Wenn ja, mittels welcher?	
3. Welche Auswirkungen hatte das Fehlen einer repressiven Rechtsgrundlage zur verdeckten Online-Durchsuchung auf das Verfahren?	

Vielen Dank!

2.4. Verdeckte Teilnahme an geschlossenen Chats[90]

Bitte pro repressiver oder präventiver Teilnahme an einem geschlossenen Chat, die erfolgte oder auch nur angedacht war, einen Bogen ausfüllen.

Dienststelle:

telefonische Erreichbarkeit:

I. Allgemeine Informationen	
6. Welche Anhaltspunkte lagen vor, dass eine verdeckte Teilnahme an einem geschlossenen Chat für das Verfahren bzw. die Abwehr einer Gefahr förderlich sein könnte [bitte alle benennen]?	
7. Die verdeckte Teilnahme an einem geschlossenen Chat wurde	nur angedacht (weiter bei VI.) durchgeführt (weiter bei 3.)
8. Welche Maßnahmen gingen der Teilnahme an dem geschlossenen Chat **voraus** [bitte alle benennen]?	
9. Welche Maßnahmen wurden **im Anschluss** an die Teilnahme an dem geschlossenen Chat durchgeführt [bitte alle benennen]?	
II. Rechtsgrundlage(n) zur Teilnahme an einem geschlossenen Chat	
1. Auf welche Rechtsgrundlage(n) wurde die Anordnung der Maßnahme gestützt?	§§ 161, 163 StPO (Generalklausel) § 100a StPO § 110a StPO Präventive Norm, und zwar … Sonstige Rechtsgrundlage, und zwar …
2. Wie wurde der richterliche Beschluss begründet, sofern ein solcher erforderlich war?	
III. Betreten des geschlossenen Chats	

[90] Verdeckt im Sinne einer Nichtoffenlegung des polizeilichen Zwecks; geschlossen = zugangsgeschützt.

1. Wie haben Sie von der Existenz des geschlossenen Chats erfahren?	
6. Welche Sicherungsmechanismen hatten die Chatroombetreiber zur Zugangskontrolle ergriffen [bitte möglichst genau benennen]?	
7. Wie haben Sie das Passwort oder sonstige Zugangsdaten zu dem geschlossenen Chat erlangt?	
8. Wie haben Sie sonstige Sicherungs-mechanismen überwunden (z.B. Angaben zu Personalien, persönliche Einladung)?	
9. Wurde nach der Polizeizugehörigkeit gefragt?	Ja Nein
10. Haben Sie einen Nickname benutzt, aus dem eine Zugehörigkeit zur Polizei erkenn-bar wurde?	Ja Nein
11. Ergaben sich sonstige Probleme?	
IV. Aufenthalt in dem geschlossenen Chat	
6. Wie häufig und wie lange haben Sie sich in dem geschlossenen Chat aufgehalten?	Mal für durchschnittlich: unter einer Stunde eine bis fünf Stunden mehr als fünf Stunden
7. Welche Sicherungsmechanismen hatten die Chatroombetreiber bzw. -teilnehmer zur Kontrolle **während** des Aufenthalts in dem geschlossenen Chat ergriffen?	
8. Wie haben Sie diese überwunden?	
9. Wurde das Handeln der anderen Chat-teilnehmer in dem geschlossenen Chat **lediglich beobachtet**?	Ja Nein (weiter bei 6.)
Wenn ja, hatte **das bloße Beobachten** einen Mehrwert für [Mehrfachnennungen möglich]	... das Anlassverfahren bzw. die Abwehr einer Gefahr? Ja Nein ... andere Ermittlungsverfahren (Zufallsfunde)? Ja

	Nein
10. War es zur Erkenntnisgewinnung notwendig, deliktsspezifische Themen **aktiv** anzusprechen?	Ja Nein
Wenn ja, welche?	
11. Welche Maßnahmen wurden in dem geschlossenen Chat ergriffen (z.B. Speichern von Inhalten, Protokollieren der Kommunikation, ...) [bitte alle benennen]?	
12. Ergaben sich sonstige Probleme bei der Teilnahme?	
V. Erfolg der Maßnahme	
1. Hatte die Teilnahme an dem geschlossenen Chat Mehrwert für [Mehrfachnennungen möglich]	... das Anlassverfahren bzw. die Abwehr einer Gefahr? Ja Nein ... andere Ermittlungsverfahren (Zufallsfunde)? Ja Nein
2. Wurden die in dem geschlossenen Chat gewonnenen Erkenntnisse als Beweismittel in ein Gerichtsverfahren eingebracht?	
Wenn ja, wie (z.B. Protokollverlesung, Zeugenbeweis)?	
3. Hätten die Erkenntnisse, die durch die Teilnahme an dem geschlossenen Chat gewonnen wurden, auch mittels anderer Maßnahmen gewonnen werden können?	Ja Nein
Wenn ja, mit welchen [bitte alle benennen]?	
VI. Angedachte, aber nicht durchgeführte Maßnahmen *Nicht auszufüllen, wenn die Maßnahme durchgeführt wurde*	
1. Welche Maßnahmen gingen der angedachten Teilnahme an dem Chat **voraus** [bitte alle benennen]?	

2. Auf welche Rechtsgrundlage(n) sollte die Anordnung der angedachten Maßnahme gestützt werden?	§§ 161, 163 StPO (Generalklausel) § 100a StPO § 110a StPO Präventive Norm, und zwar … Sonstige Rechtsgrundlage, und zwar …
3. Warum wurde die Maßnahme nicht durchgeführt?	Abgelehnter richterl. Beschluss (weiter bei4.) Sonstige Gründe, und zwar …
4. Warum wurde der Erlass eines Beschlusses abgelehnt?	

Vielen Dank!

2.5. Verdeckter Zugriff auf zwischengespeicherte Daten

Hierunter ist der Zugriff auf Daten **ohne Mitwirkung des Netzbetreibers** zu verstehen, wenn die Daten

a) weder unmittelbar beim Urheber der Daten noch der Person, für die die Daten bestimmt sind, gespeichert sind, beispielsweise
- Zugriff auf E-Mails weder beim Empfänger noch beim Absender, also z.B. beim Provider
- Zugriff auf zugangsgeschützte Speichermöglichkeiten im Internet (z.B. Webspace, Storage System, Webhosting oder Nethosting)

oder

b) in einem für Entwürfe vorgesehenen Ordner des E-Mail-Postfachs, auf das mehrere Personen zugriffsberechtigt sind, gespeichert sind.

Bitte pro repressivem oder präventivem Zugriff, der erfolgte oder auch nur beantragt wurde,
einen Bogen ausfüllen.

Dienststelle:

telefonische Erreichbarkeit:

I. Allgemeine Informationen	
10. Welche Anhaltspunkte lagen vor, dass ein verdeckter Zugriff auf zwischengespeicherte Daten für das Verfahren bzw. die Abwehr einer Gefahr förderlich sein könnte [bitte alle benennen]?	
11. Welche Maßnahmen gingen dem verdeckten Zugriff auf die Daten **voraus** [bitte alle benennen]?	
12. Für den Fall, dass ein Zugriff erfolgte, welche Maßnahmen wurden **im Anschluss** durchgeführt [bitte alle benennen]?	
II. Rechtsgrundlage(n) für den verdeckten Zugriff auf zwischengespeicherte Daten	
13. Auf welche Rechtsgrundlage(n) wurde der **Antrag** auf verdeckten Zugriff auf die	

Daten gestützt?	
14. Wurde ein richterlicher Beschluss abgelehnt, sofern ein solcher erforderlich war?	Ja Nein
Wenn ja, mit welcher Begründung?	
15. Auf welche Rechtsgrundlage(n) wurde der **Beschluss** gestützt, sofern ein solcher erforderlich war?	
16. Wurde bei der Ermächtigungsgrundlage danach differenziert, ob die E-Mails gelesen oder ungelesen waren, sofern der Zugriff auf E-Mails erfolgte?	Ja Nein
Wenn ja, welche Rechtsgrundlage(n) wurde a) für gelesene E-Mails b) für ungelesene E-Mails angenommen?	 a) b)
17. Wurde bei der Rechtsgrundlage danach differenziert, auf welchem Speichermedium die Daten zwischengespeichert waren?	Ja Nein
Wenn ja, welche Rechtsgrundlage(n) wurde für die verschiedenen Speichermedien angenommen ?	
III. Durchführung des verdeckten Zugriffs	
14. Ist ein Zugriff erfolgt?	Ja (weiter bei 3.) Nein (weiter bei 2.)
15. Wenn nein, warum nicht?	
16. Wie haben Sie von der Existenz der Daten erfahren?	
17. Wie gelang der Zugriff auf die zwischen-gespeicherten Daten?	
18. War eine unbewusste Mitwirkung des Tat-verdächtigen erforderlich (z.B. Öffnen eines E-Mail-Anhanges)?	Ja Nein
Wenn ja, welcher Art?	
19. Wurde für den Zugriff der (Service-) Provider kontaktiert?	Ja Nein

Wenn ja, welche Probleme ergaben sich hierbei [bitte alle benennen]?	
20. Waren (sonstige) Begleitmaßnahmen für den Zugriff erforderlich?	Ja Nein
Wenn ja, welche?	
21. Wie oft wurde auf die Daten zugegriffen?	Mal
22. Das Speichermedium befand sich [soweit bekannt]	im Inland im Ausland
23. Ergaben sich sonstige Probleme bei der Durchführung?	
IV. Erfolg	
1. Hatte der verdeckte Zugriff auf die Daten einen Mehrwert für [Mehrfachnennungen möglich]	... das Anlassverfahren bzw. die Abwehr einer Gefahr? Ja Nein ... andere Ermittlungsverfahren (Zufallsfunde)? Ja Nein
2. Wurden die verdeckt gewonnen Daten als Beweismittel in ein Gerichtsverfahren eingebracht?	Ja Nein
Wenn ja, wie (z.B. Protokollverlesung, Zeugenbeweis)?	
3. Hätten die Erkenntnisse, die durch den verdeckten Zugriff auf die Daten gewonnen wurden, auch mittels anderer Maßnahmen gewonnen werden können?	Ja Nein
Wenn ja, mittels welcher Maßnahmen [bitte alle benennen]?	

Vielen Dank!