Jan Ziekow/Alfred G. Debus/Dieter Katz/Alexander Niestedt/Axel Piesker/Corinna Sicko

Verdeckte Datenerhebungsmaßnahmen in der polizeilichen Praxis

Ergebnisse der Evaluation gemäß § 100 Polizei- und Ordnungsbehördengesetz Rheinland-Pfalz

Speyerer Forschungsberichte 290

Jan Ziekow / Alfred G. Debus / Dieter Katz /
Alexander Niestedt / Axel Piesker / Corinna Sicko

VERDECKTE DATENERHEBUNGSMASSNAHMEN IN DER POLIZEILICHEN PRAXIS

Ergebnisse der Evaluation gemäß § 100 Polizei- und Ordnungsbehördengesetz Rheinland-Pfalz

DEUTSCHES FORSCHUNGSINSTITUT
FÜR ÖFFENTLICHE VERWALTUNG

2018

Gefördert durch die Bundesrepublik Deutschland und die Länder

Bibliografische Information der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.ddb.de abrufbar.

(Speyerer Forschungsberichte ; 290)
ISBN 978-3-941738-28-7

Herstellung:
**DEUTSCHES FORSCHUNGSINSTITUT
FÜR ÖFFENTLICHE VERWALTUNG**

Umschlagentwurf:

© 8/97 TRIFTY ART Grafik Design • 67550 Worms • Hauptstr. 32 • Tel.: 0 62 41/95 15 38

Vorwort

An dieser Stelle ist allen Projektbeteiligten zu danken. Dazu gehören insbesondere die Mitarbeiterinnen und Mitarbeiter der fünf Polizeipräsidien und des Landeskriminalamts, die die Erhebungsbögen im Evaluationszeitraum ausgefüllt haben. Unser Dank geht darüber hinaus an die unterschiedlichen Gesprächspartner in den Polizeibehörden, an die für die POG-Maßnahmen zuständigen Richterinnen und Richter des Oberverwaltungsgerichts sowie an die Vertreter der Hochschule für Polizei, die für weitergehende Fragen zur Verfügung standen. Nicht zuletzt gilt der Dank unserer zentralen Ansprechpartnerin im Ministerium des Innern und für Sport, Frau Dr. *Martina Baunack*, für die sehr gute und konstruktive Zusammenarbeit.

Im März 2018

Jan Ziekow
Alfred G. Debus
Alexander Niestedt
Axel Piesker
Corinna Sicko

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1. Einleitung

Die Pflicht zur Evaluation einzelner Maßnahmen zur verdeckten Datenerhebung wurde in § 100 POG erstmals durch das Landesgesetz zur Änderung des Polizei- und Ordnungsbehördengesetzes und anderer Gesetze v. 2.3.2004 (GVBl. S. 202) eingeführt. Nach Abs. 1 S. 1 hatte die Landesregierung über die Wirksamkeit der Maßnahmen der Sicht- und Anhaltekontrollen im öffentlichen Verkehrsraum, des sog. „Großen Lauschangriffs", der Telekommunikationsüberwachung und der sog. „Rasterfahndung" zu berichten. Während hinsichtlich der Anhalte- und Sichtkontrollen eine Gesamtschau der Wirksamkeit der Maßnahmen über eine Vielzahl von Einzelmaßnahmen vorzunehmen war, standen bei den übrigen Maßnahmen die mit den polizeilichen Handlung verbundenen teilweise intensiven Grundrechtseingriffe im Vordergrund. Die Evaluation war unabhängig von den jährlichen Berichtspflichten bei Wohnraumüberwachungen gemäß § 29 Abs. 7 POG und Telekommunikationsüberwachungen gemäß § 31 Abs. 7 S. 2 POG.[1]

Der daraufhin am 27.05.2010 vorgelegte Evaluationsbericht der Landesregierung schließt mit folgendem Gesamtfazit: „Aufgrund der vorstehend dargestellten Ergebnisse ist aus polizeilicher Sicht festzustellen, dass sich die Regelungen der §§ 9a Abs. 4, 29 und 31 POG bewährt haben. Die Vorschriften sind praxisgerecht und greifen in die Rechte der Bürgerinnen und Bürger nicht unverhältnismäßig ein. Nach einer in Aussicht genommenen Überarbeitung dieser Vorschriften sowie des § 38 POG im Rahmen der anstehenden Novellierung des POG besitzt Rheinland-Pfalz verfassungsrechtlich unbedenkliche und die praktische Polizeiarbeit unterstützende Vorschriften. Die öffentliche Sicherheit und Ordnung und der Schutz der Bürgerinnen und Bürgern kann damit auch künftig gewährleistet werden."[2]

Durch das Siebte Landesgesetz zur Änderung des POG v. 15.02.2011 (GVBl. S. 26) erhielt die Evaluierungsklausel des § 100 POG – von einer Namensergänzung zum LfDI abgesehen – ihre heutige Gestalt. § 100 Abs. 1 S. 1 POG enthält eine Pflicht der Landesregierung, dem Landtag über die Wirksamkeit der Maßnahmen bestimmter verdeckter Datenerhebungsmaßnahmen in der Zeit vom 1.4.2011 bis zum Ablauf des 31.3.2016 zu berichten. Dabei wurde die

---

1 In diesem Sinne Landesregierung, LT-Drs. 14/2287, S. 55.

2 Landesregierung, LT-Drs. 15/5615, S. 9.

Evaluierungspflicht in Bezug auf den sog. „Großen Lauschangriff“, die Telekommunikationsüberwachung in Bezug auf deren Inhalte und Umstände und die sog. „Rasterfahndung“ beibehalten. Außerdem wurden durch das Gesetz insbesondere die Telekommunikationsüberwachung um die sog. Quellen-TKÜ in § 31 Abs. 3 POG erweitert, die Auskunft über Nutzungsdaten gemäß § 31b POG, die sog. Online-Überwachung gemäß § 31c POG sowie die Funkzellenabfrage gemäß § 31e POG eingeführt und die Evaluierungspflicht in § 100 POG auf diese Maßnahmen erstreckt.[3]

Gleichzeitig wurde in § 100 Abs. 2 POG festgelegt, dass die Anfertigung des Berichts der Landesregierung unter Mitwirkung einer Stelle erfolgt, die eine wissenschaftlich fundierte Überprüfung der Maßnahme gewährleistet. Als Beispiel wurde in der Gesetzesbegründung die Deutsche Universität für Verwaltungswissenschaften Speyer genannt. Durch die Mitwirkung einer Stelle, die eine wissenschaftlich fundierte Überprüfung der Maßnahme gewährleistet, wird der Forderung einer Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18.3.2010 nach validen und strukturierten Daten Rechnung getragen[4]: „Die Mitwirkung umfasst die Erstellung eines Fragenkatalogs zur Erfassung einer aussagekräftigen Datengrundlage bis hin zur Bewertung der erhobenen Daten. Um dem Gesetzgeber eine umfassende Bewertungsgrundlage zur Optimierung bestehender Regelungen zur Verfügung zu stellen, muss der Bericht insbesondere die im künftigen § 100 Abs. 3 S. 1 POG genannten Kriterien zur Wirksamkeit der Maßnahmen darlegen und bewerten.“[5]

Der Bericht der Landesregierung muss gemäß § 100 Abs. 3 S. 1 und 2 POG Angaben insbesondere über Anlass und Zweck sowie Dauer und Ergebnis der Maßnahmen nach Abs. 1 im Berichtszeitraum enthalten, wobei personenbezogene Angaben anonymisiert werden sollen.

---

3 Vgl. Landesregierung, LT-Drs. 15/4879, S. 48.

4 Landesregierung, LT-Drs. 15/4879, S. 48.

5 Landesregierung, LT-Drs. 15/4879, S. 48.

2. Methodisches Vorgehen

Gemäß § 100 Abs. 1 POG sind folgende verdeckte Datenerhebungsmaßnahmen zu evaluieren:

- Datenerhebung durch den verdeckten Einsatz technischer Mittel in oder aus Wohnungen (sog. „großer Lauschangriff“) (§ 29 POG),
- Datenerhebung durch den Einsatz technischer Mittel zur Überwachung und Aufzeichnung der Telekommunikation, Auskunft über die Telekommunikation (Telekommunikationsüberwachung/Quellen-TKÜ) (§ 31 POG),
- Auskunft über Nutzungsdaten (§ 31b POG),
- Datenerhebung durch den Einsatz technischer Mittel in informationstechnischen Systemen (sog. Online-Durchsuchung) (§ 31c POG),
- Funkzellenabfrage (§ 31e POG),
- besondere Formen des Datenabgleichs (sog. „Rasterfahndung“) (§ 38 POG).

Da die zu untersuchenden Regelungen bereits in Kraft[6] sind (und im Evaluationszeitraum[7] nur unwesentlich modifiziert worden sind[8]), ist das Evaluationsvorhaben als retrospektive Gesetzesfolgenabschätzung (rGFA) konzipiert. Die rGFA dient dazu, die Zielerreichung einer Rechtsvorschrift im Nachhinein zu erfassen sowie intendierte und nicht-intendierte Effekte zu identifizieren, um auf Grundlage dieser Erkenntnisse den Novellierungsbedarf und -umfang festzustellen. Darüber hinaus werden im Rahmen der rGFA neben der Untersuchung des Zielerreichungsgrads noch weitere Prüfkriterien für die Bewertung der Regelungen herangezogen. Eine besondere Bedeutung kommt in

---

6 §§ 29, 31, 38 POG wurden mit dem Landesgesetz zur Änderung des Polizei- und Ordnungsbehördengesetzes und anderer Gesetze vom 02.03.2004 (GVBl. S. 2004, S. 202) eingeführt. §§ 31b, 31c, 31e wurden mit dem Siebten Landesgesetz zur Änderung des Polizei- und Ordnungsbehördengesetzes vom 15.02.2011 (GVBl. 2011, S. 26) eingeführt.

7 Der Evaluationszeitraum begann am 15.02.2011 und endete am 31.03.2016. Im April 2017 unterrichtete die Landesregierung den Landtag über die Ergebnisse der Evaluation gemäß § 100 POG (LT-Drs. 17/2752).

8 Landesgesetz zur Änderung des LIFG und datenschutzrechtlicher Vorschriften vom 20.12.2011 (GVBl. 2011, S. 427); Achtes Landesgesetz zur Änderung des POG vom 20.12.2013 (GVBl. 2013, S. 537).

dieser Untersuchung dabei der Eingriffsintensität (Eingriffsbreite und Eingriffstiefe)[9], der Geeignetheit, der Erforderlichkeit, der Akzeptanz und der Praktikabilität zu.[10]

Zur Bewertung der Wirkungen und Folgen der POG-Regelungen ist es erforderlich, die ausgewählten Prüfkriterien mit Hilfe empirisch erhobener Daten abzugleichen. Hierbei bietet sich die Durchführung einer ex-post-Analyse an, bei der nach Inkrafttreten der Regelungen geprüft wird, welche Wirkungen sich auf die vorher festgelegten Prüfkriterien ergeben. Dabei sollte auch der Einfluss von gesetzesunabhängigen Entwicklungen untersucht werden. Diese Analysemethode kommt immer dann zum Einsatz, wenn es vor Inkrafttreten der Neuregelung keine Regelung gab, eine Regelung erweitert wurde oder Daten aus der Zeit vor Inkrafttreten der untersuchten Regelung – wenn überhaupt – nur mit erheblichem Aufwand zur Verfügung gestellt bzw. erhoben werden können.[11]

Beispielsweise lässt sich anhand der Fallzahlenanalyse[12] feststellen, ob bzw. wie oft die zu untersuchenden Regelungen im Evaluationszeitraum zur Anwendung gekommen sind (z.B. Wohnraumüberwachung, Funkzellenabfrage). Für die Bewertung der Eingriffstiefe und -breite der Maßnahmen werden jedoch noch weitere Daten benötigt (z.B. Anzahl der betroffenen Personen, Anzahl der betroffenen Dritten, Art und Umfang sowie Weiterverwendung der personenbezogenen Daten). Zur Bewertung der Wirksamkeit werden darüber hinaus *Daten* zum Erfolg der jeweiligen Maßnahme sowie zum konkreten Nutzen der mit ihrer Hilfe gewonnenen *Informationen* erhoben.

Bei der Durchführung eines solchen Evaluationsvorhabens sind ein interdisziplinärer Untersuchungsansatz sowie ein Mixed-Method-Design, in dem sowohl auf quantitative als auch auf qualitative Erhebungsmethoden zurückgegriffen wird, zwingend erforderlich. Aus diesem Grund liegt der hier durchgeführten Evaluation das nachfolgend näher dargestellte Untersuchungsdesign zugrunde, das im Wesentlichen aus drei Teilen (rechtswissenschaftliche Analyse, empirisch-sozialwissenschaftliche Analyse sowie Synthese und Bewertung der in den in ersten beiden Teilen gewonnenen Ergebnisse) besteht.

---

9 *Ziekow/Debus/Piesker*, Gesetzesevaluationen, S. 104-114.

10 *Ziekow/Debus/Piesker*, Gesetzesevaluationen, S. 34.

11 *Ziekow/Debus/Piesker*, Gesetzesevaluationen, S. 37-40.

12 *Ziekow/Debus/Piesker*, Gesetzesevaluationen, S. 60.

Die **rechtswissenschaftliche Analyse** umfasst zwei Untersuchungsschritte. Zunächst wird ein Rechtsvergleich sowohl mit präventiv-polizeirechtlichen Regelungen anderer Bundesländer als auch geheimdienstlichen sowie repressiv-strafprozessualen Regelungen auf Bundesebene durchgeführt. Auf diese Weise werden Unterschiede und Gemeinsamkeiten hinsichtlich der Regelungsinhalte und -techniken sichtbar. Darüber hinaus lassen sich auch erste Anhaltspunkte bezüglich möglicherweise problematischer Regelungsstrategien und -komplexe gewinnen. Im Anschluss erfolgt eine eingehende rechtliche, insbesondere verfassungsrechtliche Prüfung der zu evaluierenden Normen. In diesem Zusammenhang wird besonderes Gewicht auf die Frage der Verhältnismäßigkeit gelegt, da diesem Punkt angesichts der teilweise gravierenden Eingriffe in besonders sensible Grundrechtsgewährleistungen erhebliches Gewicht zuzumessen ist. Ziel der rechtswissenschaftlichen Untersuchung ist es, juristische Probleme, die sich beim Vollzug der POG-Normen ergeben können, zu identifizieren.

Die **empirisch-sozialwissenschaftliche Analyse**, die aus zwei Untersuchungsschritten besteht, beschäftigt sich vor allem mit den Auswirkungen der POG-Normen in der Praxis. In einem *ersten Schritt* wurden in Abstimmung mit den sechs rheinland-pfälzischen Polizeibehörden Erhebungsbögen für alle zu evaluierenden POG-Normen entwickelt, mit denen die im Evaluationszeitraum durchgeführten Erhebungsmaßnahmen gemäß § 100 POG erfasst wurden. Da eine einfache Fallzahlenerhebung an dieser Stelle nicht ausreichend ist, um den Besonderheiten der jeweiligen Regelungen Rechnung zu tragen, war es darüber hinaus erforderlich, weitere qualitative Aspekte zu erfassen, die für die Bewertung der POG-Maßnahmen relevant sind. Die Erfassung der im Evaluationszeitraum abgeschlossenen Maßnahmen ermöglichte einerseits eine Aussage über die tatsächliche Anwendung der Regelungen (Fallzahlenanalyse). Andererseits konnten Erkenntnisse (z.B. über mögliche Probleme oder parallel durchgeführte Datenerhebungsmaßnahmen) zu der jeweils durchgeführten Maßnahme gewonnen werden. Erhoben wurden Daten zur Vorgehensweise bei der Durchführung der verdeckten Datenerhebungsmaßnahmen (Anlass/Gefahrenlage, vorher durchgeführte Maßnahmen, Vorkehrungen zur Sicherstellung des Kernbereichsschutzes), zur Anzahl der durch die Datenerhebung betroffenen Personen, zur Art der erhobenen Daten, zum Umfang der durchgeführten Maßnahme (z.B. Zahl der überwachten Telekommunikationsverbindungen, Dauer der Befristung), zu möglichen Anwendungsproblemen, zur Weiterverwendung der im Rahmen der Maßnahme erhobenen Daten, zum Erfolg der Maßnahme sowie zum Umgang mit der Unterrichtung der durch die verdeckte Datenerhebung betroffenen Personen.

Die begleitende Erfassung der Fallzahlen erfolgte durch die fünf Polizeipräsidien Koblenz, Mainz, Rheinpfalz, Trier und Westpfalz sowie durch das Landeskriminalamt (LKA) für vorher festgelegte Erhebungszeiträume. Die erste Phase der Evaluation umfasste die Zeiträume 1. August bis 30. November 2012, 1. Dezember 2012 bis 30. März 2013 sowie 1. April bis 30. September 2013. Da die begleitende Datenerhebung erst am 1 August 2012 und damit knapp eineinhalb Jahre nach Inkrafttreten der Neuregelungen beginnen konnte, erfolgte darüber hinaus eine rückwirkende Erhebung der in der Zeit zwischen dem 15. Februar 2011 und 31. Juli 2012 durchgeführten POG-Maßnahmen, um eine lückenlose Erfassung im gesamten ersten Evaluationszeitraum zu gewährleisten. Nach Abschluss der ersten Phase entschloss sich der Gesetzgeber, den Evaluationszeitraum bis zum 31. März 2016 zu verlängern, so dass die zweite Phase folgende zusätzliche Zeiträume für die begleitende Erhebung umfasste: 01. April bis 30. September 2015 und 01. Oktober 2015 bis 31. März 2016. Darüber hinaus erfolgte eine rückwirkende Erhebung der in der Zeit zwischen dem 01. Oktober 2013 und dem 31. März 2015 durchgeführten POG-Maßnahmen, um auch für den gesamten zweiten Evaluationszeitraum eine lückenlose Erfassung zu gewährleisten.

In einem *zweiten Schritt* wurden im Mai, Juni und Juli 2013 (erste Phase) mit Vertretern der sechs Polizeibehörden sowie der Hochschule der Polizei leitfadengestützte Gruppeninterviews geführt. Die Auswahl der Teilnehmer für die Gruppeninterviews erfolgte durch die jeweilige Polizeibehörde. Hierfür wurde – aufbauend auf den Ergebnissen der Datenerhebung aus dem ersten Untersuchungsschritt – ein Interviewleitfaden entwickelt. In der zweiten Evaluationsphase wurde aufgrund der sehr geringen Fallzahlen auf eine erneute, für die Polizeibehörden aufwändige Befragung im Rahmen von leitfadengestützten Interviews in Absprache mit dem Auftraggeber verzichtet. Stattdessen wurden die bereits in der ersten Phase befragten Akteure gebeten eine schriftliche Stellungnahme abzugeben. Mit Hilfe der qualitativen Interviews und der schriftlichen Stellungnahmen wurden zusätzliche Informationen gewonnen, um mögliche Probleme im Zusammenhang mit der Anwendung der POG-Regelungen näher untersuchen zu können. Dies war auch deshalb erforderlich, da der Großteil der Maßnahmen – mit Ausnahme des § 31 POG und des § 31b POG – von den Polizeibehörden bis dato noch nicht genutzt wurde. Aus diesem Grund wurden im Rahmen der Interviews sowie der schriftlichen Stellungnahmen folgende Punkte angesprochen:

- Nutzen der Datenerhebungsmaßnahmen,
- Anwendungserfahrungen und Optimierungsmöglichkeiten,
- Benachrichtigungspflichten,

- einheitliche Gerichtszuständigkeit,
- weiterer Regelungsbedarf.

Da das Oberverwaltungsgericht (OVG) in Koblenz seit der Novellierung des POG im Jahr 2011 für den Großteil der zu evaluierenden POG-Maßnahmen die Anordnungskompetenz besitzt, findet auch die Perspektive der zuständigen Richterinnen und Richter in der Evaluation Berücksichtigung. Die Einbeziehung des OVG trägt dazu bei, mögliche Probleme, die aus Sicht des Gerichts im Zusammenhang mit der Anwendung der POG-Normen aufgetreten sind, zu identifizieren. Hierzu wurde dem 7. Senat des OVG sowohl für die erste als auch für die zweite Evaluationsphase ein Fragenkatalog mit der Bitte um Stellungnahme übersandt, der folgende Punkte umfasste:

- Vorgehen bei Anträgen zur Durchführung der Datenerhebungsmaßnahmen,
- mögliche Probleme beim derzeitigen Beantragungsverfahren,
- Qualität der Anträge,
- Anwendungserfahrungen und Optimierungsmöglichkeiten,
- einheitliche Gerichtszuständigkeit für die POG-Maßnahmen.

Im **dritten Teil** der Evaluation wurden die Ergebnisse der rechtswissenschaftlichen und empirisch-sozialwissenschaftlichen Analyse zusammengeführt und einer abschließenden Bewertung unterzogen. Auf Grundlage dieser Erkenntnisse wurden zentrale Problembereiche identifiziert und damit Hinweise für Optimierungsbedarfe im Bereich der POG-Normen gegeben.

Ziel dieser retrospektiven Gesetzesfolgenabschätzung ist es, die Wirksamkeit und die Auswirkungen der POG-Regelungen unter besonderer Berücksichtigung der datenschutzrechtlichen Folgen zu ermitteln und zu bewerten. Des Weiteren zielt das Vorhaben darauf ab, Schwachstellen zu identifizieren, um Verbesserungsmaßnahmen innerhalb und außerhalb regulativer Vorschriften zu ermöglichen.

3. Rechtswissenschaftliche Analyse

3.1 Evaluationsrelevante Normierungen

3.1.1 Überblick

Durch das Siebte Landesgesetzes zur Änderung des POG v. 15.02.2011 (GVBl. S. 26) wurden die zu evaluierenden Maßnahmen in § 100 Abs. 1 S. 1 POG festgelegt:

- Datenerhebung durch den verdeckten Einsatz technischer Mittel in oder aus Wohnungen (§ 29 POG), S. 9,
- Überwachung und Aufzeichnung der Telekommunikation (§ 31 Abs. 1, 2 POG), S. 11,
- Quellen-Telekommunikationsüberwachung (§ 31 Abs. 3 POG), S. 13,
- Auskunft über Nutzungsdaten (§ 31b POG), S. 14,
- Datenerhebung durch den Einsatz technischer Mittel in informationstechnischen Systemen (§ 31c POG, sog. Online-Durchsuchung), S. 14,
- Funkzellenabfrage (§ 31e POG), S. 15,
- Besondere Formen des Datenabgleichs (§ 38 POG, sog. Rasterfahndung), S. 16.

Der Schutz des Kernbereichs privater Lebensgestaltung wurde in § 39a POG neu aufgenommen, der Schutz zeugnisverweigerungsberechtigter Berufsgeheimnisträger in § 39b POG. Die bisher bestehende Regelung in § 29 POG wurde insoweit gestrichen.[13]

Im Jahre 2011 wurde die bisherige Zuständigkeit für Entscheidungen über die Anordnung verdeckter Ermittlungsmaßnahmen nach den §§ 29, 31, 31b, 31c, 31d und 31e POG von den Amtsgerichten auf das OVG Koblenz verlagert: „Für diese Fälle soll durch die Verlagerung der bisherigen Zuständigkeit der Amtsgerichte auf das Oberverwaltungsgericht Rheinland-Pfalz die Wirksamkeit des Richtervorbehalts akzentuiert werden, da für die richterliche Beurteilung derart intensiver Grundrechtseingriffe profunde Kenntnisse des Verfassungs- und Verwaltungsrechts sowie entsprechende Erfahrungen förderlich sind.“[14]

---

13 Landesregierung, LT-Drs. 15/4879, S. 30.

14 Landesregierung, LT-Drs. 15/4879, S. 30.

Außerdem stehen die zu evaluierenden, verdeckten Datenerhebungsmaßnahmen im untrennbaren Zusammenhang mit der Pflicht zur Benachrichtigung der Betroffenen zur Erlangung effektiven Rechtsschutzes. Dementsprechend sind diese Benachrichtigungspflichten in einigen Bundesländern auch bei den einzelnen Maßnahmen mitgeregelt, während diese in Rheinland-Pfalz in § 40 Abs. 5 und 6 POG allgemein geregelt sind.

Da die Bestimmungen über den Schutz des Kernbereichs (§ 39a POG), den Schutz der Berufsgeheimnisträger (§ 39b POG) und der Benachrichtigung Betroffener (§ 40 Abs. 5, 6 POG) mit den nach § 100 POG zu evaluierenden Normen in engen Zusammenhang stehen, sind sie von diesen nicht abtrennbar. Die rechtswissenschaftliche Analyse bezieht daher im Folgenden auch diese Normen ein. In einigen Fußnoten finden sich auch Bestimmungen des BKAG und der StPO. Dies liegt daran, dass die Bestimmungen der Länder ähnlich formuliert und die rechtlichen Probleme daher ähnlich gelagert sind.

3.1.2 Datenerhebung durch den verdeckten Einsatz technischer Mittel in oder aus Wohnungen (§ 29 POG)

Die Datenerhebung durch den verdeckten Einsatz technischer Mittel in oder aus Wohnungen ist in § 29 POG geregelt und wird zumeist als (präventive) Wohnraumüberwachung oder als „Großer Lauschangriff“ bezeichnet. Die aktuelle Fassung nach dem Achten Landesgesetz zur Änderung des Polizei- und Ordnungsbehördengesetzes vom 20.12.2013 (GVBl. 2013, S. 537) basiert im Wesentlichen auf der Neufassung durch das Sechste Landesgesetz zur Änderung des Polizei- und Ordnungsbehördengesetzes v. 24.07.2005 (GVBl. 2005 S. 320). Anlass für die Neufassung war das Bundesverfassungsgerichtsurteil vom 3.3.2004, worin die Regelungen der StPO zur Wohnraumüberwachung teilweise für verfassungswidrig erklärt wurden. Aus der Urteilsbegründung ergab sich gesetzlicher Änderungsbedarf hinsichtlich der Ausgestaltung der präventiven Wohnraumüberwachung nach § 29 POG, insbesondere im Hinblick auf die Bestimmung zum Schutz des unantastbaren Kernbereichs privater Lebensgestaltung, der vom BVerfG der Menschenwürde zugeordnet wird. Zu dessen Schutz wurden Erhebungs-, Überwachungs- und Verwertungsverbote sowie Löschungspflichten aufgenommen und die Verfahrensrechte der Betroffenen gestärkt. Wesentliche Neuerung war dabei die Aufnahme einer begleitenden gerichtlichen Kontrolle der Maßnahme, um einen effektiven

Rechtsschutz zu gewährleisten und andererseits die präventive Wohnraumüberwachung als notwendige Maßnahme zur Abwehr dringender Gefahren zu erhalten.[15]

Im Laufe des Gesetzgebungsverfahrens zum Sechsten Landesgesetz zur Änderung des Polizei- und Ordnungsbehördengesetzes v. 24.07.2005 (GVBl. 2005 S. 320) wurde die Frist für die maximale Dauer der erstmaligen Anordnung einer Wohnraumüberwachung gemäß § 29 Abs. 7 S. 3 POG von zwei Monaten[16] – entsprechend einem Antrag der CDU-Fraktion – auf drei Monate erhöht. Begründet wurde dies mit der Beibehaltung der bisherigen Dreimonatsfrist, der Berücksichtigung der Vorgaben des BVerfG nach einem „überschaubaren Zeitraum“ und der ansonsten meist obligatorischen Zweitanordnung, weil eine Wohnraumüberwachung „mit hochkonspirativer Vor- und Nachbereitung in Form von Begleitmaßnahmen (taktische, technische Planung und Ausführung, z.B. durch Ermittlung des richtigen Zeitpunkts und Orts der zu installierenden Technik, ggf. einschließlich der Deinstallation) verbunden sein muss“[17]. Eine auf zwei Monate verkürzte Frist könne dem Sinn und Zweck der Maßnahme überhaupt nicht entsprechen.[18] Dem schlossen sich die Fraktionen der SPD und FDP an, um dem Umstand Rechnung zu tragen, „dass die Anbringung der Technik zur Wohnraumüberwachung in der Regel mehrere Wochen in Anspruch nimmt und deshalb die verdeckte Maßnahme regelmäßig zeitlich deutlich nach dem Anordnungszeitpunkt beginnt. Die Befristung der Maßnahme auf höchstens drei statt zwei Monate ist daher schon unter Praktikabilitätsgesichtspunkten sinnvoll. Die Ausdehnung dieser Frist führt auch nicht zu einer Verkürzung der richterlichen Kontrolle, denn es ist dem Richter in der Praxis unbenommen, im Einzelfall eine kürzere Frist als drei Monate auch im Falle der Erstanordnung festzulegen.“[19]

2011[20] wurde aus § 29 POG der Schutz des unantastbaren Kernbereichs privater Lebensgestaltung sowie der Schutz von zeugnisverweigerungsberechtigten Berufsgeheimnisträgern aus der Bestimmung über die Wohnraumüberwachung herausgenommen und jeweils in eigenen Bestimmungen gemäß

---

15 SPD und FDP, LT-Drs. 14/3936, S. 8.

16 Landesregierung, LT-Drs. 15/4879, S. 30.

17 Fraktion der CDU, LT-Drs. 14/4278, S. 7

18 Fraktion der CDU, LT-Drs. 14/4278, S. 7.

19 Fraktionen der SPD und FDP, LT-Drs. 14/4288.

20 Siebtes Landesgesetz zur Änderung des Polizei- und Ordnungsbehördengesetzes (GVBl. 2011, S. 26).

§ 39a und § 39b POG geregelt. Die in Absatz 2 aufgezählten besonders schweren Straftaten wurden erweitert, um eine Angleichung an § 100c Abs. 2 StPO zu ermöglichen.[21] 2013[22] wurde keine Regelung zur Erhebung der Daten getroffen, sondern lediglich zu Entscheidungszuständigkeiten, nämlich zur Eilzuständigkeit der Behörden, um ursprünglich zwecks Selbstsicherung erhobene Daten für andere Zwecke zu verwenden, in § 29 Abs. 6 S. 3 POG, sowie eine Verortung der die Zuständigkeit des OVG festlegenden Regelung in den Absatz 7, um klarzustellen, dass das OVG das „Gericht" für alle Absätze des § 29 POG ist[23].Die Maßnahme ist in Rheinland-Pfalz quantitativ ohne Bedeutung. Seit dem Jahre 2005 wurde bislang nur eine einzige Wohnraumüberwachung durchgeführt und abgeschlossen.[24]

3.1.3 Überwachung und Aufzeichnung der Telekommunikation (§ 31 Abs. 1, 2 POG)

Durch das Siebte Landesgesetz zur Änderung des POG v. 15.02.2011 (GVBl. S. 26) wurde die bisherige Befugnis zur Telekommunikationsüberwachung unter Beachtung der Verfassungsrechtsprechung und technischer Entwicklungen neu und differenzierter gefasst. Dabei wurde die Befugnis zur Telekommunikationsüberwachung um die Tatbestandsalternative „zur Abwehr einer gegenwärtigen Gefahr für solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt", ergänzt.[25] Neben hochrangigen Individualrechtsgütern sollen damit ebenso die Schutzgüter der Allgemeinheit geschützt werden.[26]

---

21 Vgl. *Rühle/ Suhr*, POG, § 29 Rn. 1.

22 GVBl. 2013, S. 537.

23 Bzw. auch für vormaligen Abs. 7 (und nachherigen Abs. 6), für welchen offen war, ob die dort vorgesehene Feststellung der Rechtmäßigkeit der Maßnahme auch durch das OVG zu treffen sei; vgl. Gesetzesentwurf der Fraktionen der SPD und Bündnis 90/Die Grünen, LT-Drs. 16/2506, S. 2.

24 Vgl. Jahresbericht 2005, LT-Drs. 15/114, vgl. dagegen die Jahresberichte 2006-2010; in: LT-Drs. 15/1502, LT-Drs. 15/2236, LT-Drs. 15/3438, LT-Drs. 15/4615, LT-Drs. 15/5506, LT-Drs. 16/1202, LT-Drs. 16/2570.

25 Landesregierung, LT-Drs. 15/4879, S. 21.

26 Landesregierung, LT-Drs. 15/4879, S. 31.

Weiterhin wurde der Kreis der Verantwortlichen um den „Nachrichtenmittler“ erweitert, weil es insbesondere zur Abwehr von Gefahren der organisierten Kriminalität und des internationalen Terrorismus notwendig sein könnte, auch gegenüber diesen Personen entsprechende Maßnahmen durchzuführen.[27]

Aufgrund der Erfahrungen seit der Einführung im Jahre 2004 war bekannt, dass solche Maßnahmen zwar nur in seltenen Fällen angewendet werden, sie jedoch bei besonderen Gefahrenlagen zur Abwehr von Gefahren für hochrangige Rechtsgüter unerlässlich seien.[28] Nach den Erfahrungen der Strafverfolgung gilt dies auch für die Wohnraumüberwachung.[29]

Ebenso wie die Überwachung und Aufzeichnung der Telekommunikation ist gemäß § 31 Abs. 2 S. 1 Alt. 2 POG die Erhebung von Verkehrsdaten geregelt. Damit wird an den Sprachgebrauch des § 3 Nr. 30 TKG angeknüpft.[30] Danach sind Verkehrsdaten „Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden“. Dabei wurde die Regelung technikoffen formuliert, um zukünftigen technischen Entwicklungen Rechnung tragen zu können.[31]

Die Maßnahme wird regelmäßig angewendet. Die Zahl der betroffenen TK-Anschlüsse ist zwar bislang gering geblieben,[32] die Zahl der getroffenen Anordnungen jedoch hoch.[33] Die strafprozessuale Anordnung einer TKÜ findet in der Praxis allerdings weitaus mehr Anwendung.[34]

---

27 Landesregierung, LT-Drs. 15/4879, S. 31.

28 Landesregierung, LT-Drs. 15/4879, S. 31; vgl. auch Petri, in: Lisken/ Denninger, Handbuch, Kap. G, Rn. 240.

29 Vgl. *Schmitt*, in: Meyer-Goßner/ Schmitt, StPO, § 100c Rn. 1.

30 Landesregierung, LT-Drs. 15/4879, S. 31.

31 Landesregierung, LT-Drs. 15/4879, S. 31.

32 Vgl. die Jahresberichte 2005-2012: LT-Drs. 15/114 (keine TK-Anschlüsse 2005), LT-Drs. 15/1502 (16 TK-Anschlüsse 2006), LT-Drs. 15/2236 (keine TK-Anschlüsse 2007), LT-Drs. 15/3438 (7 TK-Anschlüsse 2008), LT-Drs. 15/4615 (keine Angaben 2009), LT-Drs. 15/5506 (11 TK-Anschlüsse 2010), LT-Drs. 16/1202 (1 TK-Anschluss 2011), LT-Drs. 16/2570 (19 TK-Anschlüsse 2012).

33 Vgl. Jahresbericht 2010, LT-Drs. 15/4615, S. 6.

34 Vgl. *Petri*, in: Lisken/ Denninger, Handbuch, Kap. G, Rn. 306 f.

3.1.4 Quellen-Telekommunikationsüberwachung (§ 31 Abs. 3 POG)

In § 31 Abs. 3 POG ist die sog. Quellen-Telekommunikationsüberwachung geregelt, wodurch die verschlüsselte Telekommunikation mittels Internettelefonie überwacht werden kann. Die Vorschrift wurde im Jahre 2011 unter Verweis auf die Rechtsprechung des BVerfG eingeführt.[35] Im Unterschied zur sonstigen Telekommunikationsüberwachung setzt die Quellen-TKÜ nach § 31 Abs. 3 POG keine gegenwärtige Gefahr, sondern eine konkrete Gefahr für hochwertige Rechtsgüter voraus. Da die technische Vorbereitung einer Quellen-TKÜ einige Zeit beanspruche, sei die Maßnahme zwar zur Abwehr gegenwärtiger Gefahren in der Regel ungeeignet, aber zur Abwehr konkreter Gefahren geeignet und erforderlich.[36] Damit werde den Anforderungen der Rechtsprechung des BVerfG genügt, wonach der heimliche Zugriff auf ein informationstechnisches System bereits dann gerechtfertigt sei, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lasse, dass die Gefahr schon in näherer Zukunft eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen.[37]

Auf Anregung von Sachverständigen wurden dabei die Nichtverantwortlichen nach § 7 POG während des Gesetzgebungsverfahrens aus dem Anwendungsbereich der Quellen-TKÜ herausgenommen.[38]

3.1.5 Mitwirkungspflichten der TK-Diensteanbieter (§ 31 Abs. 6 POG)

§ 31 Abs. 6 POG flankiert die in den Abs. 1-3 der Norm näher konkretisierten Befugnisse der Polizei zur TKÜ. Ohne die Indienstnahme privater TK-Anbieter wäre die praktische Durchführung einer TKÜ in vielen Fällen nicht möglich.[39] Die Norm erfuhr im Vergleich zu ihrer Ursprungsfassung aus dem Jahre 2003[40]

---

35 Landesregierung, LT-Drs. 15/4879, 32; BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07 und 1 BvR 595/07.

36 Landesregierung, LT-Drs. 15/4879, 32.

37 Landesregierung, LT-Drs. 15/4879, 32 unter Hinweis auf BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07 und 1 BvR 595/07, Absatz Nr. 242.

38 Fraktionen der SPD, CDU und FDP, LT-Drs. 15/5332, S. 2.

39 So zum BayPAG *Schmidbauer*, in: Schmidbauer/Steiner, Art. 34b, Rn. 40; *Hauser*, in: Honnacker u.a., PAG, Art. 34b Rn. 1.

40 LT-Drs. 14/2278.

insoweit eine Verschärfung, als die Diensteanbieter mittlerweile zum „unverzüglichen“ Handeln verpflichtet sind; dies entspricht der in § 113 Abs. 4 S. 1 TKG niedergelegten Übermittlungspflicht. Gleichzeitig wurde das Zugriffsobjekt dahingehend konkretisiert, dass nicht mehr Auskunft „über nähere Umstände der Telekommunikation“ verlangt werden kann, sondern über „Verkehrsdaten“, was eine Angleichung an die Begrifflichkeiten des TKG bedeutet, vgl. § 3 Nr. 30 TKG. Zudem wurde Satz 2 der Norm eingefügt, wodurch die Polizei ermächtigt wird, auch auf Verkehrsdaten zuzugreifen, die nach der Anordnung anfallen. Darüber hinaus wurde der ursprüngliche Verweis auf § 88 TKG a.F. durch eine umfassende Verweisung auf das TKG insgesamt ersetzt.[41]

3.1.6 Auskunft über Nutzungsdaten (§ 31b POG)

Da Telemedien[42] in einem immer größeren Umfang von der Bevölkerung genutzt werden, können die Auskünfte über Nutzungsdaten gemäß § 31b POG für die Polizei auch zur Abwehr von Gefahren von großem Nutzen sein, beispielsweise bei den zunehmenden Ankündigungen von Amoklagen oder volksverhetzender oder islamistischer Propaganda im Internet. Die 2011 eingeführte Regelung dient – wie bei § 31c POG (sog. Online-Durchsuchung) – der Abwehr einer Gefahr für Leib oder Leben einer Person oder für solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt.[43]

3.1.7 Datenerhebung durch den Einsatz technischer Mittel in informationstechnischen Systemen (§ 31c POG, sog. Online-Durchsuchung)

Ebenfalls 2011 wurde die polizeiliche Ermächtigung zum verdeckten Zugriff auf informationstechnische Systeme in § 31c POG eingeführt, damit die Methoden der Sicherheitsbehörden mit den technischen Möglichkeiten der für

---

41 Vgl. zu den Veränderungen insgesamt LT-Drs. 15/4879.

42 „Der Begriff der Telemedien ist dabei weit zu verstehen und umfasst alle elektronischen Informations- und Kommunikationsdienste, es sei denn, es handelt sich um Telekommunikation oder Rundfunk. Von dem Begriff werden beispielsweise Online- Angebote von Waren oder Dienstleistungen mit unmittelbarer Bestellmöglichkeit (insbesondere Internetauktionshäuser oder -tauschbörsen, elektronische Presse und Chatrooms), das Anbieten von Videos auf Abruf oder Suchmaschinen im Internet umfasst.“ lt. Landesregierung, LT-Drs. 15/4879, S. 35.

43 Landesregierung, LT-Drs. 15/4879, S. 35.

die Gefahr Verantwortlichen Schritt halten können. Die Befugnis sollte im Einklang mit den vom BVerfG in seinem Urteil zur Online-Durchsuchung[44] ermittelten strengen verfassungsrechtlichen Vorgaben stehen, insbes. dem Schutz des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme Rechnung tragen. Dabei wurde die Vorschrift an die Regelung des § 20k BKAG angelehnt.[45] Entsprechend diesen Vorgaben dient die Maßnahme der Abwehr von Gefahren für hochrangige Individualrechtsgüter wie Leib, Leben und Freiheit oder einer existenziellen Bedrohungslage von Rechtsgütern der Allgemeinheit.[46] Als Schwachpunkt wurde bereits im Gesetzgebungsverfahren diskutiert, dass es für die Vornahme der technischen Vorbereitungsmaßnahmen keine Befugnisnorm gibt, die beispielsweise das vorherige Betreten der Wohnung des zu Überwachenden regelt.[47] Eine praktische Anwendung der Maßnahme in Rheinland-Pfalz war bislang nicht festzustellen.[48]

3.1.8 Funkzellenabfrage (§ 31e POG)

Das Verlangen der Sicherheitsbehörden gegenüber Telekommunikations-Diensteanbietern nach Auskunft über Verkehrsdaten, die in einer bestimmten räumlich bezeichneten Funkzelle in einem bestimmten Zeitraum anfallen, wurde 2011 als Funkzellenabfrage in § 31e POG eingefügt.[49] Hinsichtlich der Maßnahmevoraussetzungen wurde im Gesetzentwurf[50] zunächst auf die Voraussetzungen der Telekommunikationsüberwachung des § 31 Abs. 1 POG

---

44 BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07 und 1 BvR 595/07, BVerfGE 120, 274 ff. – Onlinedurchsuchung.

45 Landesregierung, LT-Drs. 15/4879, S. 36.

46 Landesregierung, LT-Drs. 15/4879, S. 36, unter Hinweis auf BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07 und 1 BvR 595/07, Rn. 247.

47 Kasel (Deutsche Polizeigewerkschaft, Landesverband Rheinland-Pfalz), 41. Sitzung des Innenausschusses am 04.11.2010, Teil II, S. 19; *Stöhr* (Gewerkschaft der Polizei, Landesbezirk Rheinland-Pfalz), 41. Sitzung des Innenausschusses am 04.11.2010, S. 22; *Kugelmann* (Deutsche Hochschule der Polizei), 41. Sitzung des Innenausschusses am 04.11.2010, S. 27; *Ruthig* (Johannes Gutenberg-Universität Mainz), 41. Sitzung des Innenausschusses am 04.11.2010, S. 30.

48 Vgl. Jahresberichte 2011 und 2012: LT-Drs. 16/1202, LT-Drs. 16/2570.

49 Landesregierung, LT-Drs. 15/4879, S. 40.

50 Landesregierung, LT-Drs. 15/4879, S. 40.

verwiesen; allerdings wurde im Gesetzgebungsverfahren im Interesse größtmöglicher Normenklarheit und Normenbestimmtheit der bisherige Verweis durch die textliche Wiedergabe der Eingriffsvoraussetzungen ersetzt.[51]

3.1.9 Besondere Formen des Datenabgleichs (§ 38 POG, sog. Rasterfahndung)

§ 38 POG, der den automatisierten Abgleich personenbezogener Daten (sog. Rasterfahndung) regelt, wurde 2004 neu gefasst, um die zuvor bestehenden für die polizeiliche Praxis hohe Eingriffsschwelle der gesetzlichen Voraussetzungen zu senken.[52] Damit waren eine Rechtsangleichung mit dem Ziel der Durchführung von bundesweit abgestimmten Rasterfahndungen und eine Orientierung an den Empfehlungen einer eigens zu diesem Zweck eingesetzten Bund-Länder-Kommission bezweckt. Der Eingriff wurde als für den Einzelnen nicht besonders belastend bewertet, weil er zunächst lediglich innerhalb einer Datenverarbeitungsanlage stattfand.[53]

2011 wurden die Tatbestandsvoraussetzungen an die Anforderungen des BVerfG[54] durch Erhöhung der Gefahrenschwelle angepasst und angesichts der möglichen Vielzahl von Unbeteiligten anstelle des Behördenleitervorbehalts ein Richtervorbehalt eingeführt.[55]

3.1.10 Schutz des Kernbereichs privater Lebensgestaltung (§ 39a POG)

§ 39a POG soll das vom BVerfG entwickelte zweistufige Konzept der verfassungsrechtlichen Anforderungen zum Schutz des Kernbereichs privater Lebensgestaltung bei der Durchführung verdeckter Maßnahmen umsetzen. Auf der ersten Stufe ist darauf hinzuwirken, dass die Erhebung kernbereichsrele-

---

51 Fraktionen der SPD, CDU und FDP, LT-Drs. 15/5332, S. 1 f.

52 Landesregierung, LT-Drs. 14/2287, S. 52; Art. 1 Nr. 15 Landesgesetz zur Änderung des Polizei- und Ordnungsbehördengesetzes und anderer Gesetze v. 02.03.2004 (GVBl. S. 202).

53 Landesregierung, LT-Drs. 14/2287, S. 52, unter Hinweis auf OVG Koblenz, Beschluss vom 22.03.2002 – 12 B 103331/02.OVG (richtig lautet das Az. 12 B 10331/02 und ist unter AS RP-SL 29, 419 ff. abgedruckt).

54 BVerfG, Beschl. v. 04.04.2006 – 1 BvR 518/02.

55 Landesregierung, LT-Drs. 15/4879, S. 42.

vanter Daten, soweit informations- und ermittlungstechnisch möglich, unterbleibt. Dieses Erhebungsverbot ist in Abs. 2 und 3 beschrieben. Auf der zweiten Stufe hat der Gesetzgeber durch geeignete Verfahrensvorschriften sicherzustellen, dass dann, wenn Daten mit Bezug zum Kernbereich privater Lebensgestaltung erhoben worden sind, die Intensität der Kernbereichsverletzung und ihre Auswirkungen für die Persönlichkeit und Entfaltung der betroffenen Person so gering wie möglich bleiben, was durch § 39a Abs. 4 POG gewährleistet werden soll.[56] Im Gesetzesentwurf der Landesregierung heißt es dazu: [57] „Satz 1 bestimmt, dass die Auswertung der erhobenen Daten nur unter Sachleitung des zuständigen Oberverwaltungsgerichts Rheinland-Pfalz erfolgen darf. Eine vergleichbare Regelung enthält § 20k Abs. 7 S. 3 BKAG im Hinblick auf den verdeckten Zugriff auf informationstechnische Systeme. Durch die Vorschrift wird im Interesse des Grundrechtsschutzes gewährleistet, dass die Auswertung der erhobenen Daten durch eine unabhängige und neutrale Instanz kontrolliert wird. Das Oberverwaltungsgericht Rheinland-Pfalz leitet die Auswertung der erhobenen Daten, prüft und trifft die erforderlichen Maßnahmen."

3.1.11 Schutz von Berufsgeheimnisträgern (§ 39b POG)

Der 2011 eingeführte § 39b POG bezweckt „bei Durchführung verdeckter Maßnahmen ein absolutes Erhebungs- und Verwertungsverbot für Erkenntnisse, die dem Zeugnisverweigerungsrecht der Berufsgeheimnisträgerinnen und Berufsgeheimnisträger gemäß § 53 Abs. 1 und § 53a Abs. 1 StPO unterfallen." Dieser Schutz ist nach Abs. 2 nicht mehr gerechtfertigt, wenn der Berufsgeheimnisträger selbst für die Gefahr verantwortlich ist, welche mit der in Rede stehenden Maßnahme abgewehrt werden soll (sog. Verstrickungsregelung).[58]

---

56 Landesregierung, LT-Drs. 15/4879, S. 43 f., unter Hinweis auf BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07 und 1 BvR 595/07, Rn. 281 ff.

57 Landesregierung, LT-Drs. 15/4879, S. 44.

58 Landesregierung, LT-Drs. 15/4879, S. 45.

3.1.12 Pflichten zur Benachrichtigung der Betroffenen (§ 40 Abs. 5, 6 POG)

Die Pflichten zur Benachrichtigung der Betroffenen wurden 2004 in § 40 Abs. 5 und 6 POG neu gefasst.[59] Im Hinblick auf die in Art. 19 Abs. 4 GG gewährleistete Rechtsschutzgarantie ist die bereichsspezifische Benachrichtigungspflicht der von Maßnahmen der Datenerhebung betroffenen Personen in Fällen der verdeckten Datenerhebung für den Rechtsschutz besonders bedeutsam.[60] Dabei ist das Interesse der betroffenen Person an einer schnellstmöglichen Unterrichtung und das Interesse der Polizeibehörden an der Effektivität der verdeckten Maßnahme abzuwägen, wobei die Unterrichtung im Regelfall unverzüglich nach Abschluss der Maßnahme erfolgen soll, soweit dies ohne Gefährdung der öffentlichen Sicherheit, des Zwecks der Maßnahme, eines verdeckten Ermittlers oder einer Vertrauensperson oder deren weiterer Verwendung erfolgen kann. War eine Unterrichtung auch drei Jahre nach Abschluss der Maßnahme aus den in Satz 1 genannten Gründen nicht möglich, war der Landesbeauftragte für den Datenschutz zu unterrichten.[61]

Einen Tag nach der Neufassung von 2004 erging das Urteil des BVerfG über die Zulässigkeit der Wohnraumüberwachung zur Strafverfolgung.[62] Daraufhin wurden die Ausnahmen in Abs. 5 gestrafft und die damals durch den Landesbeauftragten für Datenschutz ausgeübte Kontrolle wurde im Anschluss an die Forderung des BVerfG durch eine unabhängige gerichtliche Kontrolle ersetzt.[63] Schließlich wurde 2011 die Benachrichtigungspflicht auf die sog. Online-Durchsuchungen nach § 31c POG und auch hinsichtlich des Personenkreises erweitert. Außerdem wurde in Abs. 5 ein S. 9 angefügt, um den praktischen Bedürfnissen Rechnung zu tragen für den Fall, dass mehrere verdeckte Maßnahmen in einem zeitlichen und sachlichen Zusammenhang durchgeführt werden.[64]

---

59 Art. 1 Nr. 15 des Landesgesetzes zur Änderung des Polizei- und Ordnungsbehördengesetzes und anderer Gesetze v. 2.3.2004 (GVBl. S. 202).

60 Landesregierung, LT-Drs. 14/2287, S. 53, unter Hinweis auf BVerfG, Beschl. v. 25.4.2001 – 1 BvR 1104/92.

61 Landesregierung, LT-Drs. 14/2287, S. 53.

62 BVerfG, Urt. v. 3.3.2004 – 1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279 ff. – akustische Wohnraumüberwachung zur Strafverfolgung.

63 Fraktionen der SPD und FDP, LT-Drs. 14/3936, S. 11 f.

64 Landesregierung, LT-Drs. 15/4879, S. 45.

Als Ausnahme von Abs. 5 entfällt die Unterrichtungspflicht nach Abs. 6 Nr. 1, wenn sich an dem auslösenden Sachverhalt ein strafrechtliches Ermittlungsverfahren gegen den Betroffenen anschließt, weil insoweit sich die Rechtsstellung nunmehr aus der StPO ergibt. Außerdem entfällt die Unterrichtungspflicht nach Nr. 2, soweit zu ihrer Durchführung weitere Daten über die betroffene Person erhoben werden müssten und dies im Interesse der betroffene Person nicht geboten erscheint, um eine erneute Datenerhebung zum Zwecke der Unterrichtung zu vermeiden. Von der Unterrichtung wird ferner nach Abs. 6 Nr. 3 abgesehen, wenn keine Aufzeichnungen mit personenbezogenen Daten erstellt oder diese unverzüglich nach Beendigung der Maßnahme vernichtet wurden, weil dann nicht die Gefahr besteht, dass Nachteile für den Betroffenen entstehen.[65]

3.2 Vergleich mit den Regelungen in anderen Bundesländern

3.2.1 Überblick

Nachdem der Musterentwurf eines einheitlichen Polizeigesetzes seit 1986 nicht mehr aktualisiert wurde, sind gerade im Bereich der Datenerhebung zum Teil sehr große Unterschiede zwischen den Regelungen der Bundesländer festzustellen. Teilweise sind aber auch einzelne Rechtsfragen – wie der Schutz des Kernbereichs privater Lebensgestaltung – durch das Grundgesetz und die Konkretisierungen durch das BVerfG[66] so detailliert vorgegeben, das die Unterschiede zwischen den Normierungen in den Bundesländern eher gering sind. Der Vergleich der gemäß § 100 POG zu evaluierenden Regelungen fokussiert daher problemorientiert auf die Gemeinsamkeiten und Unterschiede insbesondere bezüglich der materiellen Maßnahmevoraussetzungen, des zuständigen Gerichts und der Geltungsdauer der Anordnung.

In allen Bundesländern sind die Maßnahmen der präventiven Wohnraumüberwachung und der Rasterfahndung speziell normiert. Außerdem verfügen die meisten Bundesländer über Regelungen zur Überwachung der Telekommunikation, jedoch ist deren Reichweite sehr unterschiedlich ausgestaltet. Hierbei wird zwischen der Überwachung von Verkehrsdaten, des Inhalts und

65 Landesregierung, LT-Drs. 14/2287, S. 53 f.

66 Vgl. nur BVerfG NJW 1973, 891; BVerfG NJW 2004, 999, 1002; BVerfG NJW 2005, 2603, 2607; BVerfG NJW 2008, 822, 832.

von verschlüsseltem Inhalt differenziert. Die Online-Durchsuchung findet sich nur noch in Bayern und auf Bundesebene.[67]

Teil der Regelung dieser verdeckten Datenerhebungsmaßnahme sind in einigen Bundesländern spezielle Pflichten zur Benachrichtigung der Betroffenen, während diese in § 40 Abs. 5 und 6 POG allgemein geregelt sind.

In der nachfolgenden Tabelle wird ein Überblick gegeben, inwieweit andere Bundesländer eine der zu evaluierenden Datenerhebungsmaßnahmen vergleichbare Regelung enthalten. Zur Übersicht über die Details, vgl. die Synopse im Anhang.

67 Vgl. § 31c POG, Art. 34d BayPAG, §§ 6e, 6f BayVSG, § 20k BKAG.

Tab. 1: Übersicht über die mit den POG-Normen vergleichbaren Regelungen in anderen Bun-desländern[68]

	Baden-Württemberg	Bayern	Berlin	Brandenburg	Bremen	Hamburg	Hessen	Mecklenburg-Vorpommern	Niedersachsen	Nordrhein-Westfalen	Saarland	Sachsen	Sachsen-Anhalt	Schleswig-Holstein	Thüringen	BKAG	StPO
Wohnraum (§ 29 POG)	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
TKÜ (§ 31 I, II POG)	●	●		●		●	●	●	●		●		●	●	●	●	●
Quellen-TKÜ (§ 31 III POG)						●	●								●	●	
Auskunft u.a. (§ 31 VI POG)	●	●		●		●	●	●	●	●	●		●	●	●	●	
Nutzungs-daten (§ 31b POG)	●			●						○				○	●	●	
Online-Durchsu-chung (§ 31c POG)		●														●	
Funkzellen-abfrage (§ 31e POG)	●	●				●								●		●	●
Rasterfahn-dung (§ 38 POG)	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

Legende: ● = entsprechende Regelung vorhanden

○ = auf einige Nutzungsdaten beschränkte Auskunftsverlangen

68 Quelle: Eigene Recherche

3.2.2 Datenerhebung durch den verdeckten Einsatz technischer Mittel in oder aus Wohnungen (§ 29 POG)

3.2.2.1 Maßnahmevoraussetzungen

Nach den Vorgaben des Art. 13 Abs. 4 S. 1 GG bedarf es für eine präventive Wohnraumüberwachung „dringender Gefahren für die öffentliche Sicherheit, insbesondere einer gemeinen Gefahr oder einer Lebensgefahr". Dieser Wortlaut wurde von § 29 Abs. 1 S. 1 POG als Voraussetzung für die nach den §§ 4 und 5 POG Verantwortlichen und unter den Voraussetzungen des § 7 POG über die dort genannten Personen übernommen. Darüber hinaus setzt das POG in Bezug auf Kontakt- und Begleitpersonen[69] die Verhinderung von besonders schweren Straftaten voraus, die in einem Katalog gesondert aufgezählt sind. Straftatenkataloge als Maßnahmevoraussetzung gibt es auch in Berlin, Brandenburg, Niedersachen, in der StPO und im BKAG.[70] Die Vorschrift orientiert sich inhaltlich an den Bestimmungen zum großen Lauschangriff in der StPO (§ 100c-e StPO),[71] der sich wiederum auf Art. 13 Abs. 3 und 5 GG stützt.

In acht Bundesländern wird eine Gefahr für eine Person vorausgesetzt[72], während in vier Bundesländern zusätzlich die Sicherheit des Bundes oder eines Landes[73] zur Wohnraumüberwachung berechtigen kann.

---

69 Zum Begriff vgl. § 26 Abs. 3 S. 2 POG.

70 Vgl. § 25 Abs. 1 S. 1; § 17 Abs. 3 ASOG Bln; § 33a Abs. 1 S. 1 BbgPolG; § 10 Abs. 1 S. 1 Nr. 2, § 1 Abs. 4 PolDVG HA; § 2 Nr. 10 i.V.m. § 35a Abs. 1 Nr. 2 Nds. SOG; § 20h Abs. 1 Nr. 1 b i.V.m. § 4a Abs. 1 S. 2 BKAG; § 100c Abs. 2 StPO.

71 Vgl. *Roos/Lenz*, POG, § 29 Rn. 1.

72 Vgl. § 25 Abs. 4 S. 1 ASOG Bln; § 15 Abs. 4 S. 1 HSOG; § 34b Abs. 1 Satz1 SOG M-V; § 18 Abs. 1 S. 1 PolG NRW: wenn/soweit das/dies „zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person" unerlässlich/erforderlich ist. Enger § 28a Abs. 1 SPolG, § 17 Abs. 4 SOG LSA, § 185 Abs. 3 LVwG: „wenn dies zur Abwehr einer gegenwärtigen Gefahr für Leib oder Leben einer Person unerlässlich ist."
Vgl. auch § 33 Abs. 2 BremPolG: „wenn dies erforderlich ist zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person, wenn Tatsachen die Annahme rechtfertigen, dass sich die Person, der die Gefahr droht oder von der die Gefahr ausgeht, in der Wohnung aufhält und die Gefahr auf andere Weise nicht abgewehrt werden kann".

73 Vgl. Art. 34 Abs. 1 S. 1 BayPAG: „wenn dies erforderlich ist zur Abwehr einer dringenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person".

Darüber hinaus existieren teilweise noch explizite Regelungen, welche den Charakter der Wohnraumüberwachung als ultima ratio sicherstellen sollen.[74]

Während in Rheinland-Pfalz die Maßnahme nur in oder aus Wohnungen des Betroffenen durchgeführt werden kann, ermöglicht § 100c StPO unter strengeren Voraussetzungen die Maßnahme auch in Wohnungen, die nicht dem Betroffenen zuzurechnen sind.[75] Die Vorschrift in Rheinland-Pfalz bleibt damit hinter dem durch das BVerfG für zulässig erachteten Rahmen[76] zurück. In den meisten Bundesländern darf die Wohnraumüberwachung auch durchgeführt werden, wenn Dritte unvermeidbar betroffen sind,[77] wohingegen im Saarland und in Thüringen eine entsprechende Regelung fehlt.

Anders als in Rheinland-Pfalz ist in einigen Ländern ausdrücklich die Befugnis normiert, im Vorfeld der Maßnahme die Wohnung zu betreten, wenn dies zur polizeilichen Aufgabenerfüllung unerlässlich ist[78] bzw. wenn dies erforderlich ist, um die technischen Voraussetzungen der Maßnahme zu schaffen.[79]

---

§ 23 Abs. 1 S. 1 PolG BW: „wenn andernfalls die Abwehr einer unmittelbar bevorstehenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leben, Gesundheit oder Freiheit einer Person gefährdet oder erheblich erschwert würde“.
§ 10a Abs. 1 S. 1 PolDVG HA: „wenn dies zur Abwehr einer dringenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person erforderlich ist“.
Wohl am weitesten sind die Voraussetzungen gemäß § 41 Abs. 1 S. 1 SächsPolG: „wenn dies zur Abwehr einer dringenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leben, Gesundheit oder Freiheit einer Person oder für bedeutende Sach- oder Vermögenswerte erforderlich ist und wenn die Erfüllung der polizeilichen Aufgaben auf andere Weise gefährdet oder erheblich erschwert werden würde“.

74 Z.B. in Hamburg gemäß § 10a Abs. 1 S. 2 Nr. 1 PolDVG HA, wonach „die Gefahr nicht anders abgewehrt werden kann“.

75 Vgl. *Schmitt*, in: Meyer-Goßner/ Schmitt, StPO, § 100c Rn. 12.

76 Vgl. BVerfG, Urt. v. 3.3.2004 – 1 BvR 2378/98, Rn. 262.

77 Vgl. Art. 34 Abs. 3 S. 3 BayPAG; § 23 Abs. 1 S. 2 PolG BW; § 25 Abs. 2 S. 2 ASOG Bln; § 33a Abs. 2 S. 6 BbgPolG; § 33 Abs. 1 S. 2 BremPolG; § 10 Abs. 1 S. 3 PolDVG HA; § 15 Abs. 2 S. 3 HSOG; § 33 Abs. 3 SOG M-V; § 35 Abs. 1 S. 2 Nds. SOG i.V.m. § 2 Nr. 10 Nds. SOG, § 18 Abs. 1 S. 2 PolG NRW; § 29 Abs. 1 S. 3 POG; § 41 Abs. 1 S. 3 SächsPolG; § 17 Abs. 3 S. 2 SOG LSA; § 185 Abs. 4 LVwG; § 20h Abs. 2 S. 3 BKAG; § 100c Abs. 3 S. 3 StPO.

78 Vgl. § 15 Abs. 7 HSOG.

79 Vgl. § 41 Abs. 2 SächsPolG; § 35 Abs. 3 S. 2 ThürPAG.

3.2.2.2 Richtervorbehalt

Entsprechend den Vorgaben des Art. 13 Abs. 4 S. 1 GG ist eine Wohnraumüberwachung grundsätzlich nur auf Grund richterlicher Anordnung zulässig. Bei Gefahr im Verzug ist eine vorherige richterliche Entscheidung in allen Bundesländern entbehrlich, jedoch unverzüglich nachzuholen.[80] Ebenfalls entfällt der Richtervorbehalt, wenn technische Mittel ausschließlich zum Schutz der bei einem polizeilichen Einsatz in Wohnungen tätigen Personen verwendet werden.[81] Für eine anderweitige Verwertung der Erkenntnisse ist allerdings wieder ein Richtervorbehalt normiert. Die Vorschriften sind insoweit an Art. 13 Abs. 5 GG angelehnt.

Im Zusammenhang mit dem Richtervorbehalt ist zugleich das zuständige Gericht geregelt. In den meisten Ländern ist das Amtsgericht zuständig,[82] in Baden-Württemberg, Brandenburg und Nordrhein-Westfalen das Landgericht.[83] Einzigartig ist demgegenüber die Zuständigkeit des OVG nach § 29 Abs. 7 POG.

---

80 So § 23 Abs. 3 S. 8 und 9 PolG BW; Art. 34 Abs. 4 S. 1 BayPAG; § 25 Abs. 5 S. 1 und S. 3 ASOG Bln; § 33a Abs. 4 S. 1 BbgPolG; § 33 Abs. 3 S. 7 und 8 BremPolG; § 10a Abs. 3 S. 7 und 8 PolDVG HA; § 15 Abs. 5 S. 1 und 7 HSOG; § 34b Abs. 5 S. 2 SOG M-V; § 35a Abs. 5 S. 1 und 5 Nds. SOG; § 18 Abs. 2 S. 5 und 6 PolG NRW; § 29 Abs. 6 S. 3 POG; § 28a Abs. 2 S. 5 SPolG; § 41 Abs. 3 S. 2 SächsPolG; § 17 Abs. 5 S. 1 und 8 SOG LSA; § 186 Abs. 1 S. 2 und 5 LVwG; § 35 Abs. 4 S. 2 und 3 ThürPAG.

81 Vgl. § 23 Abs. 4 PolG BW; Art. 34 Abs. 8 BayPAG; § 25 Abs. 6 ASOG Bln; § 33a Abs. 8 BbgPolG; § 33 Abs. 8 BremPolG; § 10a Abs. 8 PolDVG HA; § 15 Abs. 6 HSOG; § 34 Abs. 4 SOG M-V; § 35a Abs. 6 Nds. SOG; § 18 Abs. 5 PolG NRW; § 29 Abs. 6 POG; § 28a Abs. 3 SPolG; § 41 Abs. 4 SächsPolG; § 17 Abs. 6 SOG LSA; § 186 Abs. 1 S. 7 LVwG; § 35 Abs. 7 S. 1 ThürPAG.

82 Art. 34 Abs. 4 S. 2 HS 2 BayPAG; § 25 Abs. 5 S. 2 ASOG Bln; § 33 Abs. 3 S. 2 BremPolG; § 10a Abs. 3 S. 10 PolDVG HA; § 15 Abs. 5 S. 2 HSOG; § 34b Abs. 5 S. 3 i.V.m. § 34 Abs. 3 S. 3 SOG M-V; § 35a Abs. 4 S. 1 Nds. SOG; § 28a Abs. 2 S. 4 i.V.m. § 20 Abs. 1 S. 2 SPolG; § 41 Abs. 12 i.V.m. § 38 Abs. 12 S. 2 SächsPolG; § 17 Abs. 5 S. 2 SOG LSA § 186 Abs. 2 S. 1 LVwG; § 36 Abs. 6 S. 1 ThürPAG.

83 § 23 Abs. 3 S. 1 PolG BW; § 33a Abs. 4 S. 2 BbgPolG; § 18 Abs. 2 S. 1 PolG NRW.

Im Saarland und in Sachsen ist das Amtsgericht zuständig, in dessen Bezirk die Wohnung liegt bzw. in dessen Bezirk die Maßnahme überwiegend durchgeführt werden soll.[84] Ansonsten ist zumeist das Amtsgericht zuständig, in dessen Bezirk die beantragende Polizeidienststelle ihren Sitz hat[85], in Berlin das Amtsgericht Tiergarten[86]. Allerdings soll in Niedersachsen nach einer Verlängerung auf insgesamt sechs Monate das Landgericht – mit Beschwerde zum OLG – entscheiden.[87]

Auch in Baden-Württemberg, Brandenburg, Nordrhein-Westfalen und Rheinland-Pfalz war früher das Amtsgericht zuständig.[88] Heute sind dort die Landgerichte zuständig, in dessen Bezirk die beantragende Polizeibehörde ihren Sitz hat, bzw. in Rheinland-Pfalz das Oberverwaltungsgericht. Bereits 1996 hat Brandenburg für die verdeckte Datenerhebung das Landgericht für zuständig erklärt, in dessen Bezirk die beantragende Polizeibehörde ihren Sitz hat.[89]

---

84 § 28a Abs. 3 S. 3 i.V.m. § 20 Abs. 1 S. 2 SPolG sowie § 41 Abs. 12 i.V.m.. § 38 Abs. 12 S. 2 SächsPolG.

85 So Art. 34 Abs. 4 S. 2 Halbsatz 2 BayPAG; § 33 Abs. 3 S. 2 BremPolG; § 15 Abs. 5 S. 2 HSOG; § 34b Abs. 5 i.V.m. § 34 Abs. 3 S. 3 SOG M-V; § 35a Abs. 4 S. 1 Nds. SOG; § 17 Abs. 5 S. 2 SOG LSA; § 186 Abs. 2 S. 1 LVwG. In diesem Sinne auch § 10 Abs. 2 S. 10 PolDVG HA, wonach das einzige im Stadtstaat vorhandene Amtsgericht für zuständig erklärt wird.

86 So § 25 Abs. 5 S. 2 ASOG Bln.

87 Vgl. § 35a Abs. 4 S. 6 Nds. SOG.

88 § 23 Abs. 2 S. 1 PolG BW in der Fassung der Bekanntmachung v. 13.01.1992 (GBl. S. 1).
§ 18 Abs. 3 S. 5 PolG NRW in der Fassung der Bekanntmachung v. 25.07.2003 (GV NRW S. 441).
§ 29 Abs. 10 S. 1 POG in der Fassung der Änderung durch Art. 1 Gesetz v. 25.07.2005 (GVBl. S. 320).

89 Vgl. § 33 Abs. 5 S. 3 BbgPolG, Gesetz zur Neuordnung des Polizeirechts im Land Brandenburg v. 19.03.1996 (GVBl. I S. 74).

Diese Regelung wurde im Jahr 2006 für die Wohnraumüberwachung übernommen[90] und dabei der Grundrechtsschutz durch Verfahren betont.[91] In Baden-Württemberg wurde die Änderung[92] damit begründet, dass „ein Gleichklang mit der Regelung der gerichtlichen Anordnung bei der strafprozessualen Wohnraumüberwachung hergestellt (vgl. § 100d StPO)“ werden solle. [93]

In Nordrhein-Westfalen wurde die Neufassung im Jahre 2010[94] folgendermaßen begründet: „Diese besondere Kammer ist bisher bereits zuständig für die Anordnung und sonstige Entscheidungen bei der strafprozessualen Wohnraumüberwachung gemäß §§ 100c, 100d StPO. Wegen der besonderen Schwere des Eingriffs soll die Entscheidung künftig durch ein richterliches Kollegialorgan getroffen werden; zugleich wird damit Gleichklang mit den strafprozessualen Normen hergestellt.“[95]

Für die Verlagerung der bisherigen Zuständigkeit der Amtsgerichte auf das Oberverwaltungsgericht in Rheinland-Pfalz wurde in der Gesetzesbegründung[96] eine Akzentuierung der Wirksamkeit des Richtervorbehalts angeführt,

> *„da für die richterliche Beurteilung derart intensiver Grundrechtseingriffe profunde Kenntnisse des Verfassungs- und Verwaltungsrechts sowie entsprechende Erfahrungen förderlich sind. Dieser Zielsetzung trägt die Übertragung von Entscheidungen über die Anordnung verdeckter Ermittlungsmaßnahmen nach Maßgabe der vorbezeichneten Vorschriften an die Verwaltungsgerichtsbarkeit Rechnung. In Anlehnung an die in dem Koalitionsvertrag auf Bundesebene zwischen CDU, CSU und FDP getroffene Vereinbarung, dass künftig für die Entscheidung über die Anordnung der verdeckten Ermittlungsmaßnahmen nach dem Abschnitt zur Gefahrenabwehr gegen den internationalen Terrorismus im Bundeskriminalamtgesetz zur Verstärkung der Rechtsstaatlichkeit der Entscheidung nicht mehr eine Richterin*

---

90 Vgl. § 33a BbgPolG, eingefügt durch Viertes Gesetz zur Änderung des Brandenburgischen Polizeigesetzes v. 18.12.2006 (GVBl. I, S. 188).

91 Landesregierung, LT-Drs. 2/1235, S. 99.

92 Gesetz zur Änderung des Polizeigesetzes v. 18.11.2008 (GBl. S. 390).

93 Landesregierung, LT-Drs. 14/3165, S. 55.

94 Artikel 1 des Gesetzes zur Änderung des Polizeigesetzes des Landes Nordrhein-Westfalen v. 09.02.2010 (GV. NRW. S. 132).

95 Landesregierung, LT-Drs. 14/10089, S. 31.

96 Landesregierung, LT-Drs. 14/4679, S. 26.

> *oder ein Richter des Amtsgerichts am Sitz des BKA, sondern eine Richterin oder ein Richter am Bundesgerichtshof durch Vermittlung der Generalbundesanwältin oder des Generalbundesanwalts zuständig sein soll, wird die Anordnungsbefugnis nach Absatz 6 Satz 1 für die nach Absatz 3 erforderliche richterliche Anordnung ebenfalls nicht einem erstinstanzlichen Gericht, sondern dem höchsten (Landes-)Gericht des Gerichtszweiges zugewiesen."*[97]

Zu beachten ist allerdings, dass im BKAG, an dem sich der Landesgesetzgeber orientieren wollte, nach § 20v Abs. 2 BKAG das Amtsgericht weiterhin zuständig ist.

3.2.2.3 Gefahr im Verzug und laufende Unterrichtung

In allen Bundesländern ist geregelt, dass bei Gefahr im Verzug ein Richtervorbehalt zunächst nicht erforderlich ist. Allerdings ist unverzüglich eine richterliche Bestätigung der Maßnahme einzuholen. Während einige Länder allgemein den Polizeivollzugsdienst oder die Polizei[98] in Eilfällen für zuständig erklären, ist in anderen Vorschriften der Dienststellenleiter oder Behördenleiter[99] bzw. der Polizeipräsident[100] zuständig. Sachsen erklärt den Leiter des Landeskriminalamts oder einer Polizeidirektion für zuständig[101]. Schleswig-Holstein sieht die Anordnung des Leiters des Landespolizeiamtes, des Landeskriminalamtes oder einer Polizeidirektion vor[102]. In Baden-Württemberg bedarf es der Anordnung durch die Leitung eines regionalen Polizeipräsidiums, des Polizeipräsidiums „Einsatz" oder des Landeskriminalamts[103]. In Baden-Württemberg, Niedersachsen, im Saarland und in Schleswig-Holstein kann die An-

---

97 Landesregierung, LT-Drs. 15/4879 S. 30.

98 Vgl. § 25 Abs. 5 S. 3 ASOG Bln; § 33 Abs. 3 S. 7 BremPolG; § 15 Abs. 5 S. 8 HSOG; § 17 Abs. 5 S. 8 SOG LSA.

99 Vgl. Art. 34 Abs. 4 S. 1 BayPAG; § 33a Abs. 4 S. 1 BbgPolG; § 34b Abs. 5 S. 2 SOG M-V; § 35a Abs. 5 S. 3 Nds. SOG; § 18 Abs. 2 S. 4 PolG NRW; § 28a Abs. 2 S. 5 SPolG; § 35 Abs. 4 S. 2 ThürPAG.

100 Vgl. § 10a Abs. 3 S. 7 PolDVG HA.

101 Vgl. § 41 Abs. 3 S. 2 SächsPolG.

102 § 186 Abs. 1 S. 3 LVwG.

103 § 23 Abs. 3 S. 8 i.V.m. § 22 Abs. PolG BW.

ordnungsbefugnis besonders beauftragten Personen, etwa Beamten des höheren Dienstes, übertragen werden[104] Nach dem BKAG ist der Präsident des BKA zuständig.[105] Dagegen kann die Exekutive, gestützt auf die Wohnraumüberwachung in der StPO, keine Eilentscheidung ohne das Gericht treffen: Zuständig ist nach § 100d Abs. 1 S. 2 StPO der Vorsitzende des Landgerichts, dies als Folge des Art. 13 Abs. 3 GG.

Nur wenige Länder sehen darüber hinaus noch eine fortlaufende Unterrichtung des Gerichts über die durchgeführten Maßnahmen der Wohnraumüberwachung vor.[106] In welchen Abständen die Polizeibehörden das Gericht zu unterrichten haben, bestimmt das Gericht selbst.[107]

3.2.2.4 Befristung der Maßnahme

Alle Länder sehen vor, dass die Maßnahme in der richterlichen Anordnung zu befristen ist, wobei eine Verlängerung möglich ist. Lediglich die Zeiträume der Befristung und Verlängerung sind unterschiedlich. Die Befristung der Maßnahme reicht von höchstens vier Wochen[108], einem Monat[109] über zwei Monate[110] bis hin zu höchstens drei Monaten.[111] Auch die Verlängerung der Maß-

---

104 Vgl. § 23 Abs. 3 S. 8 i.V.m. § 22 Abs. 6 S. 2 PolG BW; § 35a Abs. 5 S. 4 Nds. SOG; §§ 28a Abs. 2 S. 5 HS. 1 SPolG, § 186 Abs. 1 S. 4 LVwG.

105 Vgl. § 20h Abs. 3 S. 1 BKAG.

106 Vgl. § 25 Abs. 5 S. 10 Bln ASOG; § 10a Abs. 4 S. 1 PolDVG HA; § 34b Abs. 6 S. 1 SOG M-V; § 29 Abs. 4 S. 1 POG; § 17 Abs. 5a S. 1 SOG LSA; § 186a Abs. 6 S. 1 LVwG.

107 Vgl. BVerfG: Urteil v. 3.3.2004 – 1 BvR 2378/98, Rn. 279.

108 In Bremen und Hamburg – jeweils auch für Verlängerungen – § 33 Abs. 3 S. 5 und 6 BremPolG; § 10a Abs. 3 S. 5 und 6 PolDVG HA.

109 In Bayern, Brandenburg, Niedersachsen, Nordrhein-Westfalen, Saarland, Sachsen und Thüringen - jeweils auch für Verlängerungen, vgl. Art. 34 Abs. 4 S. 4 BayPAG, § 33a Abs. 4 S. 5 und 6 BbgPolG, § 35a Abs. 4 S. 2 HS 2, S und 5 Nds. SOG, § 18 Abs. 2 S. 2 und 4 PolG NRW, § 28a Abs. 2 S. 2 und 3 SPolG; § 41 Abs. 5 S. 2 und 3 SächsPolG, § 35 Abs. 5 S. 2 und 3 ThürPAG.

110 In Mecklenburg-Vorpommern und Schleswig-Holstein jeweils mit der Möglichkeit von Verlängerungen von je bis zu einen Monat, vgl. § 34b Abs. 5 S. 4 und 5 SOG M-V, § 186a Abs. 5 S. 3 und 4, LVwG.

111 In Baden-Württemberg, Rheinland-Pfalz - jeweils mit der Möglichkeit von Verlängerungen um je bis zu einen Monat, vgl. § 23 Abs. 3 S. 4 und 5 PolG BW, § 29 Abs. 3 S. 2

nahme ist beschränkt. Zulässig sind teilweise höchstens drei weitere Verlängerungen[112] bzw. Verlängerungen um höchstens vier Wochen[113] oder einen Monat.[114] Am kürzesten sind die Anordnungs- und Verlängerungsfristen in Bremen und Hamburg mit jeweils höchstens vier Wochen.[115]

Als zusätzliche verfahrensmäßige Sicherung ordnet § 35a Abs. 4 S. 6 Nds. SOG an, dass nach insgesamt sechs Monaten über die weitere Verlängerung eine Zivilkammer des Landgerichts – mit Beschwerde zum OLG – entscheidet.

3.2.2.5 Sonstiges

In allen Ländern sind die erlangten Daten aus der Wohnraumüberwachung besonders zu kennzeichnen. Eine Verwendung für andere Zwecke als der Gefahrenabwehr ist zulässig, sofern die entsprechenden Voraussetzungen vorliegen. Die Exekutive (Landesregierung, Ministerium, Senat) hat über die Maßnahmen die Länderparlamente (Landtag, Bürgerschaft, Abgeordnetenhaus) regelmäßig zu unterrichten. Nur in Sachsen-Anhalt und im BKAG ist derartiges nicht vorgesehen. Die Berichtspflicht ergibt sich insoweit unmittelbar aus Art. 13 Abs. 6 GG.

---

und 3 POG. In Berlin mit der Möglichkeit von Verlängerungen um je bis zu drei Monaten, § 25 Abs. 5 S. 7, 8 ASOG Bln. In Hessen und Sachsen-Anhalt mit der Möglichkeit von bis zu 3 Verlängerungen von je bis zu drei Monaten; § 15 Abs. 5 S. 6 und 7 HSOG; § 17 Abs. 5 S. 6 und 7 SOG LSA.

112 In Hessen und Sachsen-Anhalt, vgl. § 15 Abs. 5 S. 6, 7 HSOG; § 17 Abs. 5 S. 6, 7 SOG LSA.

113 Vgl. § 33 Abs. 3 S. 5 und 6 BremPolG, § 10a Abs. 3 S. 5 und 6 PolDVG HA.

114 In allen Bundesländern außer in Berlin, Hessen und Sachsen-Anhalt.

115 So § 33 Abs. 3 S. 5 BremPolG, § 10a Abs. 3 S. 5 und 6 PolDVG HA.

3.2.3 Überwachung und Aufzeichnung der Telekommunikation (§ 31 Abs. 1, 2 POG)

3.2.3.1 Überblick

Die Überwachung und Aufzeichnung der Telekommunikation ist in zwölf Bundesländern geregelt,[116] nicht aber in Berlin, Bremen, Nordrhein-Westfalen und Sachsen.

In einigen Ländern – darunter Rheinland-Pfalz – ist ausdrücklich normiert, dass sich die Aufzeichnung und Überwachung auf die Verkehrsdaten und die Inhalte der Telekommunikation beziehen.[117] In anderen Ländern betrifft die Überwachung und Aufzeichnung „personenbezogene Daten".[118] Darunter fallen alle Informationen über den Betroffenen, sein Verhalten und die auf ihn beziehbaren Sachverhalte.[119] Auch diese beziehen sich also auf Verkehrs- und Inhaltsdaten.[120] In Baden-Württemberg dürfen nur Verkehrsdaten erhoben werden, auf den Inhalt der Gespräche hat die Polizei insoweit keinen Zugriff.[121] Im BKAG und in der StPO heißt es, dass „die Telekommunikation" überwacht und aufgezeichnet werden darf.[122] Davon erfasst sind Bestandsdaten, Verkehrsdaten, Nutzungsdaten und Inhaltsdaten.[123]

Brandenburg verweist auf die Voraussetzungen zur Wohnraumüberwachung.[124] Häufig ist der Schutz von Berufsgeheimnisträgern und des Kernbereichs privater Lebensgestaltung wie in § 39b bzw. § 39a POG einheitlich für

---

116 Vgl. § 23a PolG BW; Art. 34a, c BayPAG; § 33b BbgPolG; § 10b-e PolDVG HA; § 15a HSOG; § 34, 34a SOG M-V; § 33a Nds. SOG; § 31 POG; § 28b SPolG; §§ 17a, 17 b SOG LSA; §§ 185a, 186 LVwG; § 34a ThürPAG.

117 Vgl. § 10b Abs. 1 PolDVG HA; § 15a Abs. 1, 2 HSGO; § 34a Abs. 2 SOG M-V; § 33a Abs. 2 Nds. SOG; § 31 Abs. 1, 2 POG; § 17b Abs. 1, 2 SOG LSA, § 185a Abs. 2 LVwG; § 34a Abs. 1 ThürPAG.

118 Vgl. Art. 34a Abs. 1 BayPAG, § 33b Abs. 1 BbgPolG, § 28b Abs. 1 SPolG.

119 Vgl. *Berner/Köhler/Käß*, BayPAG, Vor Art. 30-49, Rn. 6; vgl. auch § 3 Abs. 1 LDSG Rh-Pf.

120 Vgl. Berner/ Köhler/ Käß, BayPAG, Art. 34a Rn.7.

121 Vgl. § 23a Abs. 1 PolG BW, *Stephan/Deger*, PolG BW, § 23a Rn. 1.

122 Vgl. § 20l Abs. 1 S. 1 BKAG, § 100a Abs. 1 StPO; zum Begriff der Telekommunikation vgl. § 3 Nr. 22 TKG.

123 Vgl. *Bruns*, in: KK-StPO, § 100a Rn. 7 ff; *Graf*, in: Graf, StPO, § 100a Rn. 12-22a; *Petri*, in: Lisken/ Denninger, Handbuch, Kap. G, Rn. 335.

124 Vgl. § 33b Abs. 1 BbgPolG.

alle verdeckten Maßnahmen der Datenerhebung normiert. Darauf wird noch besonders eingegangen (→ Kapitel 3.2.11, S. 52 ff. sowie Kapitel 3.2.10, S. 50 ff.).

Die Erhebung von Geräte- und Kartennummer von mobilen Telekommunikationsendgeräten und die Ermittlung des Standortes eines mobilen Telekommunikationsendgeräts wurden in Rheinland-Pfalz eigenständig in § 31a POG normiert.[125] Die Maßnahmen wurden bislang auf § 31 POG a.F. gestützt. Die Sonderregelung trägt dem Umstand Rechnung, dass sie minder schwere Grundrechtseingriffe darstellen und die Eingriffsvoraussetzungen daher reduziert werden können.[126] Andere Bundesländer haben diese Befugnis weiterhin in ihrer Vorschrift zur Telekommunikationsüberwachung belassen, in Mecklenburg-Vorpommern sowie im Saarland und teilweise auch in Bayern ausdrücklich nur zur Vorbereitung einer TKÜ.[127]

3.2.3.2 Maßnahmevoraussetzungen

In Hessen, Niedersachsen, Sachsen-Anhalt und Schleswig-Holstein kann sich die Maßnahme nur auf eine Gefahr für eine Person stützen.[128] In Baden-Württemberg, Hamburg, Mecklenburg-Vorpommern und Rheinland-Pfalz kann die TKÜ auch durchgeführt werden, wenn die Sicherheit des Bundes oder eines

125 Vgl. Landesregierung, LT-Drs. 15/4879, S. 31; *Rühle*, POG, Kap. G, Rn. 101.

126 Vgl. Landesregierung, LT-Drs. 15/4879, S. 33.

127 Vgl. § 23a Abs. 6 PolG BW; Art. 34a Abs. 2 S. 1 BayPAG; § 33b Abs. 3 BbgPolG; § 34a Abs. 3 SOG M-V; § 28b Abs. 3 SPolG.

128 § 15a Abs. 1 S. 1 HSOG und § 17a Abs. 1 SOG LSA: „wenn dies zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person unerlässlich ist“; ähnlich § 185a Abs. 1 S. 1 LVwG.
§ 33a Abs. 1 Nds. SOG: „zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person“.

Landes bedroht ist.[129] In Bayern und Thüringen genügt sogar die gemeine Gefahr für Sachen.[130] In Brandenburg und im Saarland finden sich außerdem Umschreibungen, die (auch) auf die Verhinderung bestimmter Straftaten abstellen.[131]

Teilweise darf die Maßnahme nur durchgeführt werden, wenn sonst die Erfüllung der polizeilichen Aufgabe gefährdet oder wesentlich erschwert würde[132] bzw. die Maßnahme unerlässlich ist[133] bzw. zwingend erforderlich[134].

---

129 § 10b Abs. 1 S. 1 Nr. 1 PolDVG HA: „wenn dies zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person erforderlich ist“,
§ 34a Abs. 1 S. 1 Nr. 1 SOG MV: „wenn dies zur Abwehr einer im einzelnen Falle bevorstehenden Gefahr für Leib, Leben, Freiheit einer Person oder den Bestand oder die Sicherheit des Bundes oder eines Landes erforderlich ist“,
§ 31 Abs. 1 POG: „zur Abwehr einer gegenwärtigen Gefahr für Leib oder Leben einer Person oder für solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt“,
§ 23a Abs.1 S.1 PolG BW: „soweit bestimmte Tatsachen die Annahme rechtfertigen, dass eine konkrete Gefahr für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder eine gemeine Gefahr vorliegt”.

130 Art. 34a Abs. 1 S. 1 BayPAG: „über die für eine Gefahr Verantwortlichen, soweit dies zur Abwehr einer dringenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder für Sachen, soweit eine gemeine Gefahr besteht, erforderlich ist“,
§ 34b Abs. 1 PAG: „Die Polizei kann zur Abwehr für den Bestand oder die Sicherheit der Bunderepublik Deutschland oder eines Landes, für Leben, Freiheit oder Gesundheit einer Person oder zur Abwehr einer gemeinen Gefahr für Sachen“.

131 So § 33b BbgPolG, der auf die Voraussetzungen der Wohnraumüberwachung verweist.
§ 28b Abs. 1 S. 1 SPolG, wonach die Datenerhebung „zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person“ und „zur vorbeugenden Bekämpfung der in § 100 c der Strafprozessordnung genannten Straftaten über Personen, wenn konkrete Vorbereitungshandlungen für sich oder zusammen mit weiteren bestimmten Tatsachen die begründete Annahme rechtfertigen, dass sie diese Straftaten begehen werden“ erfolgen kann.

132 So in Baden-Württemberg: § 23a Abs. 1 S. 3 PolG BW

133 So in Hessen, Sachsen-Anhalt und Schleswig-Holstein: § 15a Abs. 1 S. 1 HSOG; § 17b Abs. 1 SOG LSA und § 185a Abs. 1 S. 1 LVwG.

134 Vgl. § 31 Abs. 2 POG.

Erleichterte Eingriffsschwellen gibt es in Bayern und Mecklenburg-Vorpommern bei Datenerhebungen über eine Person, der eine Gefahr droht.[135]

Die Maßnahmen richten sich gegen den Verantwortlichen oder Notstandspflichtigen bzw. Nichtstörer. In einigen Ländern richten sich die Maßnahmen darüber hinaus auch auf Dritte, die für die Verantwortlichen Nachrichten entgegennehmen oder weitergeben oder deren Kommunikationseinrichtungen benutzen (sog. Nachrichtenmittler).[136]

3.2.3.3 Richtervorbehalt

Hinsichtlich des Richtervorbehalts für eine Überwachung und Aufzeichnung der Telekommunikation zeigen sich Parallelen zur Wohnraumüberwachung: In allen Bundesländern mit Regelung einer Telekommunikationsüberwachung ist eine vorherige richterliche Entscheidung nur bei Gefahr im Verzug entbehrlich.[137] Wie auch bei den übrigen zu evaluierenden Vorschriften ist für die richterlichen Anordnungen einheitlich das OVG Rheinland-Pfalz zuständig.[138] In den übrigen Bundesländern ist das Amtsgericht zuständig, in dessen Bezirk die beantragende Polizeidienststelle ihren Sitz hat.[139]

---

135 Art. 34a Abs. 3 S. 1 BayPAG: „Die Polizei kann bei Gefahr für Leben oder Gesundheit einer Person 1. durch die Überwachung und Aufzeichnung der Telekommunikation personenbezogene Daten über diese Person erheben“,
§ 34a Abs. 1 S. 1 Nr. 2 SOG M-V: Daten erheben über „Personen, wenn deren Leben oder Gesundheit gefährdet ist“.

136 Vgl. Art. 34a Abs. 1 S. 1 Nr. 2 BayPAG, § 10b Abs. 1 S. 1 Nr.2 PolDVG HA, § 31 Abs. 1 Nr. 2 POG, § 17b Abs. 3 S. 1 Nr. 2 SOG LSA, § 34a Abs. 1 S. 1 Nr. 2 und 3 ThürPAG, § 20l Abs. 1 S. 1 Nr. 3, 4 BKAG, § 100a Abs. 3 StPO.

137 So Art. 34c Abs. 1 S. 1 Halbs. 2 BayPAG; § 33b Abs. 5 S. 1 BbgPolG, § 10e Abs. 1 S. 2 PolDVG HA; § 15a Abs. 5 S. 1 HSOG; § 34a Abs. 4 S. 2 SOG M-V; § 33a Abs. 5 S. 1 Nds. SOG, § 31 Abs. 5 S. 3 POG; § 28b Abs. 4 S. 4 SPolG; § 17b Abs. 4 S. 1 SOG LSA; § 186 Abs. 1 S. 2 LVwG; § 34a Abs. 5 S. 2 ThürPAG.

138 § 31 Abs. 5 S. 1 POG; vgl. Landesregierung, LT-Drs. 15/4879 S. 33.

139 So Art. 34c Abs. 1 S. 1 i.V.m. Art. 34 Abs. 4 S. 2 Halbs. 2 BayPAG; § 23a Abs. 2 S. 1 PolG BW; § 33b Abs. 5 S. 2 BbgPolG; § 10e Abs. 1 S. 5 PolDVG HA; § 15a Abs. 5 S. 2 HSOG; § 34a Abs. 7 S. 6 Halbs. 2 i.V.m. § 34 Abs. 3 S. 3 SOG M-V; § 33a Abs. 4 S. 1 Nds. SOG; § 28b Abs. 4 S. 6 Halbs. 1 SPolG; § 17b Abs. 4 S. 2 i.V.m. § 17 Abs. 5 S. 2 SOG LSA; § 186 Abs. 2 S. 1 LVwG; § 36 Abs. 6 S. 1 ThürPAG.

3.2.3.4 Befristung der Maßnahme

Weitgehende Parallelen zur Wohnraumüberwachung zeigen sich auch bei den Höchstfristen für die Durchführung einer Maßnahme. Die gleichen Fristen wie bei der Wohnraumüberwachung (Anordnung für maximal drei Monate mit höchstens dreimaliger Verlängerung für je drei Monate gelten in Hessen und Sachsen-Anhalt.[140] Ähnliches gilt für Baden-Württemberg, Hamburg, Mecklenburg-Vorpommern, Niedersachsen und Thüringen.[141] In Schleswig-Holstein ist die Maßnahme auf höchstens zwei Monate mit einer Verlängerungsmöglichkeit um jeweils nicht mehr als einen Monat zulässig.[142] In Bayern, Brandenburg und Saarland ist die Maßnahme auf höchstens einen Monat zu befristen und kann um jeweils nicht mehr als einen Monat verlängert werden.[143]

3.2.3.5 Sonstiges

In einigen Bundesländern wird der Umfang der Telekommunikationsüberwachung näher konkretisiert oder erweitert. So darf sich beispielsweise in Mecklenburg-Vorpommern, Niedersachen, Schleswig-Holstein und in Thüringen die Datenerhebung auch auf „die innerhalb des Telekommunikationsnetzes in Datenspeichern abgelegten Inhalte“ beziehen.[144]

In allen Bundesländern sind die durch die TKÜ erlangten Daten besonders zu kennzeichnen und dürfen unter bestimmten Voraussetzungen für andere Zwecke verwendet werden.

---

140 § 15a Abs. 5 S. 4 i.V.m. § 15 Abs. 5 S. 6, 7 HSOG; § 17a Abs. 4 S. 2 i.V.m. § 17 Abs. 5 S. 6, 7 SOG LSA.

141 § 23a Abs. 2 S. 6 i.V.m. § 23 Abs. 3 S. 3 und 4 PolG BW; § 10e Abs. 2 S. 3 und 4 PolDVG HA sowie § 34a Abs. 4 S. 5 und 6 SOG M-V; § 33a Abs. 4 S. 2 Halbs. 2, S. 3 Nds. SOG; § 34a Abs. 6 S. 2 und 3 ThürPAG.

142 Vgl. § 186a Abs. 5 S. 3 und 4 LVwG.

143 So Art. 34c Abs. 3 S. 4 Nr. 3 und S. 5 BayPAG; § 33b Abs. 5 S. 5 Nr. 3 und S. 6 BbgPolG; § 28b Abs. 4 S. 2 und 3 SPolG.

144 § 34a Abs. 2 Nr. 1 SOG M-V; § 33a Abs. 2 S. 1 Nr. 1 Nds. SOG; § 185a Abs. 2 Nr. 1 LVwG, § 34a Abs. 1 S. 1 ThürPAG.

Die Maßnahmen unterliegen in den meisten Bundesländern einer Berichtspflicht der Landesregierung gegenüber dem Parlament,[145] nicht aber in Bayern, Hessen und Sachsen-Anhalt.

In Hamburg findet sich eine strafrechtliche Sanktionsnorm: „Werden Maßnahmen nach §§ 10b bis 10d durchgeführt,[146] so darf diese Tatsache von Personen, die Telekommunikationsdienste erbringen oder an der Erbringung solcher Dienste mitwirken, anderen nicht mitgeteilt werden. Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer entgegen Satz 1 eine Mitteilung macht.“[147]

3.2.4 Quellen-Telekommunikationsüberwachung (§ 31 Abs. 3 POG)

Die Überwachung und Aufzeichnung der laufenden Telekommunikation erfolgt durch Eingriffe mit technischen Mitteln in die vom Betroffenen genutzten informationstechnischen Systeme. Eine spezielle Normierung der Quellen-Telekommunikationsüberwachung erfolgte überdies in Hamburg, Hessen, Thüringen und im BKAG.[148] Eine entsprechende Normierung in § 17c SOG LSA in der Fassung vom 17.10.2013 wurde vom Landesverfassungsgericht Sachsen-Anhalt für nichtig erklärt[149] und vom Landesgesetzgeber aufgehoben[150]. Die allgemeinen Bestimmungen zur TKÜ in den anderen Ländern berechtigen nach Auffassung des BVerfG nicht zur Durchführung einer Quellen-TKÜ.[151]

In allen Ländern ist sicherzustellen, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird und der Eingriff in das informationstechnische System notwendig ist, um die Überwachung und Aufzeichnung der Telekommunikation insbesondere auch in unverschlüsselter Form zu

---

145 Vgl. § 23a Abs. 10 PolG BW; § 33b Abs. 11 BbgPolG; § 10e Abs. 7 PolDVG HA; § 34a Abs. 9 i.V.m. § 34 Abs. 7 SOG M-V; § 37a Nds. SOG; § 31 Abs. 7 i.V.m. § 29 Abs. 8 S. 2 POG; § 28b Abs. 7 i.V.m. § 28a Abs. 5 SPolG; § 186b Abs. 1 S. 2 LVwG; § 36 Abs. 7 ThürPAG; § 100b Abs. 5 StPO.

146 Gemeint sind die Wohnraumüberwachung, die TKÜ und die Onlinedurchsuchung.

147 § 10e Abs. 6 S. 1 und 2 PolDVG HA.

148 Vgl. § 10c PolDVG HA; § 15b HSOG; § 34a Abs. 2 ThürPAG; § 20l Abs. 2 BKAG.

149 Vgl. LVerfG Sachsen-Anhalt, Urt. v. 11.11.2014, Az. LVG 9/13.

150 § 1 des Fünften Gesetzes zur Änderung des Gesetzes über die öffentliche Sicherheit und Ordnung des Lands Sachsen-Anhalt vom 27.10.2015 (GVBl. LSA S. 559).

151 Vgl. BVerfG NJW 2008, 822, 831.

ermöglichen. Erforderlich sind weiter bestimmte Sicherstellungen technischer Art.[152] Eine Protokollierungspflicht bestimmter Daten ist vorgeschrieben.[153]

Im Übrigen werden die Regelungen zur „einfachen“ Telekommunikationsüberwachung weitgehend übernommen.[154] In Rheinland-Pfalz genügt u.a. eine Gefahr für Leib und Leben einer Person, diese muss nicht gegenwärtig sein[155]. Während sich in Hamburg und Hessen die Maßnahme nur gegen die für eine

---

152 § 10c Abs. 2 PolDVG HA; § 15b Abs. 2 HSOG; § 31 Abs. 3 S. 3 i.V.m. § 31c Abs. 2 S. 1-2 POG: „Es ist technisch sicherzustellen, dass 1. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und 2. die vorgenommenen Veränderungen bei Beendigung der Maßnahme soweit technisch möglich automatisiert rückgängig gemacht werden. Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen.“
Darüber hinaus verlangt § 31 Abs. 3 S. 3 i.V.m. § 31c Abs. 2 S. 3 POG: „Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.“
Etwas anders § 34a Abs. 2 S. 1 und 2 ThürPAG: „Die Überwachung und Aufzeichnung kann auch in der Weise erfolgen, dass mit informationstechnischen Programmen in vom Betroffenen genutzte Systeme eingegriffen wird, wenn 1. durch technische Maßnahmen sichergestellt ist, dass ausschließlich eine laufende Telekommunikation überwacht wird und 2. der Eingriff in das informationstechnische System notwendig ist, um eine die Überwachung und Aufzeichnung in unverschlüsselter Form zu ermöglichen. Ein Zugriff auf die auf dem System gespeicherten Daten sowie alle anderen auf dem informationstechnischen System integrierten technischen Systemkomponenten ist unzulässig.“

153 § 10c Abs. 3 S. 1 PolDVG HA; § 15b Abs. 3 S. 1 HSOG: „Bei jedem Einsatz des technischen Mittels sind zum Zwecke der Datenschutzkontrolle und der Beweissicherung zu protokollieren:
1. die Bezeichnung des technischen Mittels und der Zeitraum seines Einsatzes,
2. die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,
3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und
4. die Organisationseinheit, die die Maßnahme durchführt.“

Weiter verlangen § 10c Abs. 3 S. 2 und 3 PolDVG HA und § 15b Abs. 3 S. 2 ff. HSOG: Die Protokolldaten dürfen nur verwendet werden, um der betroffenen Person oder einer hierzu befugten öffentlichen Stelle oder einem Gericht die Prüfung zu ermöglichen, ob die Maßnahme nach Absatz 1 rechtmäßig durchgeführt worden ist. Sie sind bis zum Ablauf des auf die Speicherung folgenden Kalenderjahres aufzubewahren und sodann automatisiert zu löschen, wenn sie für den in Satz 2 genannten Zweck nicht mehr erforderlich sind.“; weitgehend identisch auch § 31 Abs. 3 S. 3 i.V.m. § 31c Abs. 4 POG.

154 § 10e Abs. 1 PolDVG HA; § 31 Abs. 3 POG; vgl. § 34a Abs. 3 ThürPAG.

155 Vgl. § 31 Abs. 3 POG.

Gefahr Verantwortlichen richten darf,[156] ist die Maßnahme in Rheinland-Pfalz und Thüringen auch gegen den Nachrichtenmittler zulässig.[157]

Mit Änderungsgesetz vom 20.12.2013[158] wurde die Höchstdauer von Anordnungen wie deren Verlängerung durch eine Änderung von § 31 Abs. 4 S. 2 und 3 POG auf zwei Monate reduziert.

3.2.5 Mitwirkungspflichten der TK-Diensteanbieter (§ 31 Abs. 6 POG)

Flankierend zur eigentlichen TKÜ verpflichten die Bundesländer auch die Telekommunikationsdienstleister, die Überwachung und Aufzeichnung der Telekommunikation zu ermöglichen.[159] Sie haben auf Verlangen Auskünfte über Verkehrsdaten zu erteilen.[160] In Berlin, Bremen und Sachsen bestehen keine derartigen Regelungen. Hinsichtlich der dafür erforderlichen Entschädigung wird auf § 23 Justizvergütungs- und -entschädigungsgesetz (JVEG) verwiesen.[161]

Nur für die Bundesländer Berlin, Bremen und Sachsen waren explizite Regelungen für die Auskünfte über die Telekommunikation nicht ersichtlich. Alle Bundesländer, welche die Überwachung und Aufzeichnung der Telekommunikation normiert haben, haben auch Regelungen zu Auskünften über die Tele-

---

156 § 10c Abs. 4 PolDVG HA, § 15b Abs. 4 HSOG.

157 Vgl. § 31 Abs. 3 S. 1 POG; § 17b Abs. 2, § 34a Abs. 1 Nr. 2 und 3 ThürPAG.

158 Achtes Landesgesetz zur Änderung des Polizei- und Ordnungsbehördengesetzes vom 20.12.2013 (GVBl. 2013, S. 537).

159 Vgl. § 23a Abs. 5 PolG BW; Art. 34b Abs. 2 und 3 BayPAG; § 33b Abs. 7 S. 1 BbgPolG; § 10b Abs. 3 PolDVG HA; § 15a Abs. 1 HSOG; §§ 28a, 34a Abs. 6 S. 1 SOG M-V; § 33a Abs. 7 S. 1 Nds. SOG; § 31 Abs. 6 S. 1, 3 POG; § 28c Abs. 1 SPolG; § 17b Abs. 6 S. 1 SOG LSA; § 185a Abs. 4 S. 1 LVwG; § 34a Abs. 7 ThürPAG.

160 Vgl. § 23a Abs. 5 S. 1 und 2 PolG BW; Art. 34b Abs. 2 BayPAG; § 33b Abs. 6 BbgPolG; § 10d Abs. 4 PolDVG HA; § 15a Abs. 2 HSOG; § 34a Abs. 6 SOG M-V („Auskünfte über nähere Umstände der Telekommunikation“); § 33a Abs. 2 und 8 S. 1 und 2 Nds. SOG; § 20a PolG NRW; § 28c Abs. 1 SPolG; § 17b Abs. 6 SOG LSA („nähere Umstände der durchgeführten Telekommunikation“); § 185a Abs. 2 LVwG; § 34a Abs. 7 ThürPAG („die erforderlichen Auskünfte“).

161 § 23a Abs. 5 S. 4 PolG BW; Art. 34b Abs. 7 BayPAG; § 33b Abs. 7 S. 2 BbgPolG; § 10d Abs. 4 S. 3 PolDVG HA; § 3 Abs. 2 HSOG; § 34a Abs. 6 S. 2 SOG M-V; § 33a Abs. 7 S. 2 Nds. SOG; § 20a Abs. 5 PolG NRW; § 31 Abs. 6 S. 4 i.V.m. § 12 Abs. 5 POG; § 28b Abs. 2 iVm § 28c Abs. 5 SPolG; § 17a Abs. 3 S. 2 iVm § 17b Abs. 6 S. 2 SOG LSA; § 185a Abs. 4 S. 2 LVwG; § 34a Abs. 7 S. 3 ThürPAG.

kommunikation geschaffen und häufig gelten diese Normen auch für die Auskünfte über die Telekommunikation genauso oder zumindest weitgehend entsprechend.[162]

Als signifikante Erleichterungen der Erhebung von Verkehrsdaten gegenüber der Überwachung der Telekommunikation waren ersichtlich:

- Herabsetzung der Eingriffsschwelle gemäß § 33b Abs. 6 S. 1 BbgPolG[163],
- seltenerer Richtervorbehalt gemäß § 33b Abs. 6 S. 4 Halbs. 2 BbgPolG oder § 34 Abs. 3 S. 1 SOG M-V (vgl. § 34a Abs. 4 SOG M-V),
- erleichterte Aufzeichnung von Verkehrsdaten mit Einwilligung der Anschlussinhaberin oder des Anschlussinhabers gemäß § 33 Nds. SOG.

Gegenüber der Überwachung und Aufzeichnung der Telekommunikation gelten teilweise gesteigerte Anforderungen, wenn Auskunft darüber begehrt wird, ob von einem Telekommunikationsanschluss Telekommunikationsverbindungen zu einer bestimmten Person hergestellt worden sind (sog. Zielsuchlauf).[164]

---

162 In diesem Sinne: Art. 34b Abs. 2 BayPAG; § 33b Abs. 6 BbgPolG; § 10d Abs. 4 PolDVG HA; § 15a Abs. 2 S. 1 HSOG; § 34a Abs. 6 SOG M-V; § 33a Abs. 8 Nds. SOG; § 31 Abs. 6 POG; § 28c SPolG; § 17b Abs. 6 SOG LSA; § 185a Abs. 4 LVwG; § 34a Abs. 7 ThürPAG.

163 Für Verkehrsdaten gemäß § 33b Abs. 6 S. 1 BbgPolG: „zur Abwehr einer Gefahr für Leib, Leben oder Freiheit einer Person oder für den Bestand oder die Sicherheit des Bundes oder des Landes“.
Bei Überwachung und Aufzeichnung der Telekommunikation gemäß § 33b Abs. 1 iVm § 33a Abs. 1 BbgPolG: „wenn bestimmte Tatsachen die Annahme rechtfertigen, dass dadurch Erkenntnisse erlangt werden, die für die Gefahrenabwehr von Bedeutung sind und 1. dies zur Abwehr einer dringenden Gefahr für Leib, Leben oder Freiheit einer Person unerlässlich ist oder 2. aufgrund tatsächlicher Anhaltspunkte, insbesondere aufgrund konkreter Informationen über Planungs- und Vorbereitungshandlungen, anzunehmen ist, dass a) Mord, Totschlag oder Völkermord (§§ 211, 212 des Strafgesetzbuche oder § 6 des Völkerstrafgesetzbuches), …“.

164 Art. 34b Abs. 2 S. 2 BayPAG: „Die Übermittlung von Daten über Telekommunikationsverbindungen, die zu diesen Personen hergestellt worden sind, darf nur angeordnet werden, wenn die Erforschung des Sachverhalts oder die Ermittlung ihres Aufenthaltsorts auf andere Weise aussichtslos oder wesentlich erschwert wäre.“
§ 10d Abs. 2 PolDVG HA: „Die Erteilung einer Auskunft darüber, ob von einem Telekommunikationsanschluss Telekommunikationsverbindungen zu den in § 10b Absatz 1 genannten Personen hergestellt worden sind (Zielsuchlauf), darf nur angeordnet werden, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos wäre.“

In Baden-Württemberg und Nordrhein-Westfalen existieren nur Regelungen zu Auskünften über die Kommunikation. Die Voraussetzungen für diese Maßnahme sind mit denen der anderen Bundesländer vergleichbar.[165] § 20a Abs. 3 S. 1 PolG NRW verzichtet dabei allerdings auf einen präventiven Richtervorbehalt und lässt eine Anordnung durch die Behördenleiterin oder den Behördenleiter genügen. Demgegenüber geht § 23a Abs. 2 PolG BW – wie allgemein üblich – vom Grundsatz eines präventiven Richtervorbehalts aus. Abweichend davon darf gemäß § 23a Abs. 3 PolG BW eine Maßnahme, „die allein auf die Ermittlung des Aufenthaltsortes einer vermissten, suizidgefährdeten oder hilflosen Person gerichtet ist“, durch bestimmte Behördenvertreter erfolgen.

Die Polizeigesetze der Länder Baden-Württemberg, Bayern, Brandenburg, Hamburg, Hessen, Mecklenburg-Vorpommern, Niedersachsen, Saarland, Sachsen, Sachsen-Anhalt, Schleswig-Holstein und Thüringen sowie das BKAG und die StPO enthalten Regelungen zur Erhebung von (Telekommunikations-)Bestandsdaten i.S.v. §§ 95, 111 TKG mitsamt Beauskunftung über Daten einer Zugangssicherung und einer Zuordnung einer zu einem Zeitpunkt zugewiesenen IP-Adresse[166]; das Polizeigesetz Nordrhein-Westfalens nur zu Erhebung

---

165 § 23a PolG BW: „Der Polizeivollzugsdienst kann ohne Wissen des Betroffenen Verkehrsdaten im Sinne des § 96 Absatz 1 des Telekommunikationsgesetzes über die in den §§ 6 und 7 sowie unter den Voraussetzungen des § 9 über die dort genannten Personen erheben, soweit bestimmte Tatsachen die Annahme rechtfertigen, dass eine konkrete Gefahr für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder eine gemeine Gefahr vorliegt. Die Datenerhebung ist auch zulässig, soweit bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für eines der in S. 1 genannten Rechtsgüter hinweisen. Datenerhebungen dürfen nur durchgeführt werden, wenn sonst die Erfüllung der polizeilichen Aufgabe gefährdet oder wesentlich erschwert würde. Die Datenerhebung darf auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.“
§ 20a Abs 1 S. 2 PolG NRW: „1. wenn die hohe Wahrscheinlichkeit eines Schadens für Leben, Gesundheit oder Freiheit einer Person besteht oder 2. zur Abwehr einer gemeinen Gefahr und nur, soweit die Erreichung des Zwecks der Maßnahme auf andere Weise aussichtslos oder wesentlich erschwert wäre.“

166 § 23a Abs. 1, 9 PolG BW; Art. 34b, Abs. 4, 5, 6 BayPAG; § 33c Abs. 1, 2, 4 BbgPolG; § 10f Abs. 1, 2, 3, 5 PolDVG HA; § 15a Abs. 2 S. 2, 3, 4 HSOG; § 28a Abs. 1, Abs. 2 S. 1, Abs. 3 S. 1 SOG M-V; § 33c Abs. 1 S. 1, Abs. 2 S. 1, Abs. 3 S. 1 Nds. SOG; § 20a Abs.1 S. 1 Nr. 1, S. 2 PolG NRW; § 28c Abs. 2, 3 SPolG; § 42 Abs. 1, 2, 7 SächsPolG; § 17a Abs. 1, 2, 3 S. 1 SOG LSA; § 180a Abs. 1, 2, 3 S. 1 LVwG S-H; § 34e Abs. 1, 2 ThürPAG; § 20b Abs. 2, 3, 7 S. 1 BKAG; § 100j Abs. 1, 2, 5 S. 1 StPO.

der Bestandsdaten und der Zuordnung zu einer zu einem Zeitpunkt zugewiesenen IP-Adresse[167]. Eine Regelung über fest zugewiesene IP-Adressen findet sich lediglich in Schleswig-Holstein.[168]

3.2.6 Auskunft über Nutzungsdaten (§ 31b POG)

Anfang 2011 wurde mit § 31b POG eine Regelung für die Auskunft über Nutzungsdaten i.S.d. § 15 Abs. 1 TMG[169] eingefügt. Diesen Nutzungsdaten im Bereich der Telemedien entsprechen im Bereich der Telekommunikation im Wesentlichen die Bestandsdaten gemäß § 3 Nr. 3 TKG zuzüglich der Verkehrsdaten gemäß § 3 Nr. 30 TKG. Nachdem das BVerfG[170] mehrere Regelungen im TKG über die Abfrage von Bestandsdaten für verfassungswidrig, aber bis zum 31.6.2013 weitergeltend erklärt hatte, fügten Baden-Württemberg, Brandenburg, Nordrhein-Westfalen, Schleswig-Holstein und Thüringen im Rahmen der Neuregelung für die Bestandsdaten gemäß TKG auch Regelungen für die Erhebung von einigen Nutzungsdaten i.S.d. § 15 Abs. 1 TMG ein.

Während nach § 31b POG Auskunft über alle Nutzungsdaten i.S.d. § 15 Abs. 1 TMG verlangt werden kann, ermöglicht § 20a Abs. 3 S. 1 Nr. 3 PolG NRW lediglich die Erhebung über „Merkmale zur Identifikation der Nutzerin oder des Nutzers, Angaben über den Beginn und das Ende sowie den Umfang der jeweiligen Nutzung nach Datum und Uhrzeit“. Ähnlich begrenzt § 180a Abs. 4 LVwG die Erhebung „auf die Identifikation der Nutzer und auf das Datum und die Uhrzeit des Beginns und Endes der Nutzung beschränkte Daten“.

Voraussetzung für die Datenerhebung ist eine Gefahr für ein individuelles oder kollektives Rechtsgut[171]. Weiter ist die Datenerhebung nur zulässig, „soweit sie zwingend erforderlich ist“ (§ 31b POG) bzw. „soweit die Erreichung

---

167 § 20a Abs. 1 S. 1 Nr. 1, S. 2 PolG NRW

168 § 180a Abs. 2 S. 3 LVwG S-H.

169 § 15 Abs. 1 TMG: „Der Diensteanbieter darf personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen (Nutzungsdaten). Nutzungsdaten sind insbesondere 1. Merkmale zur Identifikation des Nutzers, 2. Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und 3. Angaben über die vom Nutzer in Anspruch genommenen Telemedien.“.

170 BVerfG, NJW 2012, 1419 ff.; s. a. die Ausführungen unter Ziff. 3.3.5.

171 § 33b Abs. 6 S. 1 BbgPolG: „zur Abwehr einer Gefahr für Leib, Leben oder Freiheit einer Person oder für den Bestand oder die Sicherheit des Bundes oder des Landes“.

des Zwecks der Maßnahme auf andere Weise aussichtslos oder wesentlich erschwert wäre“ (§ 20a Abs. 1 S. 2 PolG NRW). Baden-Württemberg verlangt gemäß § 23a Abs. 1 S. 1 PolG BW für die Erhebung von Nutzungsdaten im Sinne des § 15 Abs. 1 S. 2 Nr. 2 und 3 TMG, d. h. über Zeit und Umfang sowie Gegenstand der Telemediennutzung, eine Gefahr für ein individuelles oder kollektives Rechtsgut[172], wohingegen für die Erhebung von Nutzungsdaten im Sinne des § 15 Abs. 1 S. 2 Nr.1 TMG, d.h. über Merkmale zur Identifikation des Nutzers, eine Gefahr für die öffentliche Sicherheit genügt[173].

Normierungen zur Erhebung von (Telemedien)Bestandsdaten im Sinne von § 14 TMG finden sich in Baden-Württemberg, Brandenburg, Hamburg, Sachsen-Anhalt und Schleswig-Holstein[174].

---

§ 34b Abs. 2, Abs. 1 ThürPAG: „zur Abwehr einer Gefahr für den Bestand oder die Sicherheit der Bundesrepublik Deutschland oder eines Landes oder für Leben, Gesundheit oder Freiheit einer Person oder zur Abwehr einer gemeinen Gefahr“.
§ 20a Abs. 1 S. 2 PolG NRW „1. wenn die hohe Wahrscheinlichkeit eines Schadens für Leben, Gesundheit oder Freiheit einer Person besteht oder 2. zur Abwehr einer gemeinen Gefahr und nur, soweit die Erreichung des Zwecks der Maßnahme auf andere Weise aussichtslos oder wesentlich erschwert wäre. “;
§ 31b Abs. 1 S. 1 POG: „zur Abwehr einer Gefahr für Leib oder Leben einer Person oder für solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt,…“;
§ 180a LVwG: „soweit dies zur Abwehr einer im einzelnen Falle bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person sowie zur Abwehr einer gegenwärtigen Gefahr eines gleichgewichtigen Schadens für Sach- oder Vermögenswerte oder für die Umwelt erforderlich ist“.

172 § 23 a Abs. 1 S. 1 PolG BW „soweit bestimmte Tatsachen die Annahme rechtfertigen, dass eine konkrete Gefahr für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder eine gemeine Gefahr vorliegt“

173 § 23 a Abs. 9 S. 1 PolG BW „zur Abwehr einer Gefahr für die öffentliche Sicherheit“.

174 § 23a Abs. 9 PolG BW; § 33c Abs. 1, 2, 4 BbgPolG; § 10f Abs. 1, 2, 3, 5 PolDVG HA; § 20a Abs. 1 S. 1 Nr. 1, S. 2 PolG NRW; § 17a Abs. 1, 2, 3 S. 1 SOG LSA; § 180a Abs. 1, 2, 3 S. 2, 4 LVwG S-H.

3.2.7 Datenerhebung durch den Einsatz technischer Mittel in informationstechnischen Systemen (§ 31c POG, sog. Online-Durchsuchung)

Eine der Online-Durchsuchung gemäß § 31c POG vergleichbare Regelung besteht bislang nur in Bayern und im BKAG.[175] Da das BVerfG insoweit eine bereichsspezifische Regelung verlangt, [176] kann in den anderen Bundesländern die Maßnahme nicht auf die Datenerhebungs- oder allgemeine Generalklausel gestützt werden.[177] Die Maßnahme kommt bundesweit kaum zur praktischen Anwendung.[178] Bei der Durchsicht eines elektronischen Speichermediums nach § 110 Abs. 3 StPO handelt es sich dagegen um eine Maßnahme der offenen Datenerhebung.[179]

Die Online-Durchsuchung ist gemäß § 31c Abs. 1 POG zulässig „zur Abwehr einer Gefahr für Leib, Leben oder Freiheit einer Person oder für solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt“. Außerdem setzt die Maßnahme voraus, dass die Aufgabenerfüllung auf andere Weise nicht möglich erscheint oder wesentlich erschwert wäre.[180]

Die Bestimmung des § 20k BKAG ist teilweise mit dem Wortlaut des § 31c POG identisch, die Abweichungen sind gering. Während die Protokolldaten im POG gemäß § 31c Abs. 4 S. 3 PolG unverzüglich zu löschen sind, soweit sie für den Erhebungszweck nicht mehr erforderlich sind, können die Protokolldaten nach § 20k Abs. 3 BKAG auch noch bis zum Ablauf des folgenden Kalenderjahres aufbewahrt werden. Dies gilt auch dann, wenn sie für den Erhebungszweck nicht mehr erforderlich sind. In der schriftlichen Anordnung ist im POG das technische Mittel zu nennen; nach dem BKAG ist dies nicht erforderlich.

Nach § 20k Abs. 1 S. 2 BKAG kann die Maßnahme schon dann zulässig sein, „wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt,

---

175 Vgl. Art. 34d BayPAG, Art. 6e, f BayVSG, § 20k BKAG.

176 BVerfGE 120, 274, 315 ff.

177 Vgl. *Pieroth/ Schlink/ Kniesel*, POR, § 14 Rn. 138; vgl. auch *Petri*, in: Lisken/ Denninger, Handbuch, Kap. G Rn. 170.

178 Vgl. *Käß*, BayVBl 2010, 1, 14; *Soiné*, NVwZ 2012, 1585, 1589; *Petri*, in: Lisken/ Denninger, Handbuch, Kap. G, Rn. 354.

179 Vgl. *Schmitt*, in: Meyer-Goßner/ Schmitt, StPO, § 110 Rn. 6; *Ritter*, Vorratsdatenspeicherung, S. 232.

180 Vgl. § 31c Abs. 1 S. 2 POG und Art. 34d Abs. 1 S. 2 BayPAG.

dass ohne Durchführung der Maßnahme in näherer Zukunft ein Schaden eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für eines der in S. 1 genannten Rechtsgüter hinweisen." Eine ähnliche Formulierung hat das BVerfG verwendet.[181] Maßnahmen zur Aufklärung im Vorfeld einer Gefahr oder eine Gefahrenvorbeugung sind insoweit nicht zulässig.[182] Die Bestimmung in Rheinland-Pfalz bleibt dahinter zurück.

Inhaltlich ähnlich, aber erheblich komplexer formuliert sind die Voraussetzungen in Bayern.[183] Der Tatbestand differenziert zwischen Zugangsdaten und gespeicherten Daten, für die aber dieselben Voraussetzungen gelten. Die Zugangsdaten (Passwörter, Pin usw.) ermöglichen teilweise erst den Eingriff in das informationstechnische System. Die Erhebung von Zugangsdaten kann dabei als Vorbereitungshandlung oder als Alternative (im Zusammenhang mit einer Durchsuchung und Sicherstellung) dienen.[184] Über eine Datenerhebung und die Regelung im POG hinaus dürfen gemäß Art. 34d Abs. 1 S. 3 BayPAG auch Daten gelöscht werden, wenn eine gegenwärtige Gefahr für Leib oder Leben nicht anders abgewehrt werden kann. Weitergehend als in Bayern fin-

---

181 Vgl. BVerfG NJW 2008, 822, 831, Rn. 251. Zur verfassungskonformen Auslegung von § 20k Abs. 1 S. 2 vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1140/09, Rn. 213, 214.

182 Vgl. *Böckenförde*, JZ 2008, 925, 931.

183 Art. 34d Abs. 1 S. 1 BayPAG: „Die Polizei kann mit technischen Mitteln verdeckt auf informationstechnische Systeme zugreifen, um Zugangsdaten und gespeicherte Daten zu erheben von Personen,

1. die für eine Gefahr verantwortlich sind, soweit dies zur Abwehr einer dringenden Gefahr für a) den Bestand oder die Sicherheit des Bundes oder eines Landes, b) Rechtsgüter der Allgemeinheit, deren Bedrohung die Grundlagen der Existenz der Menschen berührt, oder c) Leib, Leben oder Freiheit einer Person erforderlich ist, oder
2. soweit bestimmte Tatsachen die begründete Annahme rechtfertigen, dass a) sie für Personen nach Nr. 1 bestimmte oder von diesen herrührende Mitteilungen entgegennehmen oder entgegengenommen haben, ohne insoweit das Recht zur Verweigerung des Zeugnisses nach §§ 53, 53a StPO zu haben, oder solche Mitteilungen weitergeben oder weitergegeben haben oder b) die unter Nr. 1 genannten Personen ihre informationstechnischen Systeme benutzen oder benutzt haben.".

184 Vgl. dazu *Schmidbauer*, in: Schmidbauer/ Steiner, BayPAG, Art. 34d Rn. 85, 97.

den sich in Rheinland-Pfalz technische Anforderungen zum Schutz der Integrität des Informationstechnischen Systems sowie zur Protokollierung der Maßnahme.[185]

Zur Vorbereitung dürfen auch die erforderlichen Daten – wie insbesondere spezifische Kennungen sowie der Standort eines informationstechnischen Systems – ermittelt werden.[186]

Die Maßnahme kann sich in Rheinland-Pfalz und in Bayern auch auf die Nachrichtenmittler erstrecken, während im BKAG nur die Verhaltens- und Zustandsverantwortlichen betroffen sind.[187]

Die Maßnahmen setzen eine richterliche Entscheidung voraus. Während in Rheinland-Pfalz das OVG zuständig ist, besteht in Bayern die Zuständigkeit einer besonderen Kammer des Landgerichts, in dessen Bezirk die beantragende Polizeidienststelle ihren Sitz hat.[188] Für Beschwerden gegen Entscheidungen des Landgerichts ist in Bayern das Oberlandesgericht, für die Maßnahme nach dem BKAG das Amtsgericht zuständig.[189] Die Maßnahmen sind auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als einen Monat (nach § 20k Abs. 6 BKAG jeweils nicht mehr als drei Monate) ist zulässig.[190]

Das BVerfG sah den Gesetzgeber als befugt an, bei Gefahr im Verzug eine Ausnahme vom Richtervorbehalt vorzusehen.[191] Dennoch sieht nur Bayern eine Sonderregelung für Gefahr im Verzug vor[192]. In Rheinland-Pfalz wurde darauf „aufgrund des zeitlichen Vorlaufs für die technische Vorbereitung der Maßnahme“ verzichtet.[193] Auch im BKAG besteht insoweit keine gesonderte Regelung.[194]

---

185 Vgl. § 31c Abs. 2 POG und § 31c Abs. 4 POG.

186 Vgl. § 31c Abs. 3 S. 1 POG und Art. 34d Abs. 2 S. 1 BayPAG.

187 Vgl. § 31c Abs. 1 S. 1 Nr. 2 POG; Art. 34d Abs. 1 S. 1 Nr. 2 BayPAG; § 20k Abs. 4 BKAG iVm § 17, 18 BPolG.

188 Vgl. Art. 34d Abs. 3 S. 3 BayPAG, § 31c Abs. 5 S. 3 POG.

189 Vgl. § 20v Abs. 2 S. 1 BKAG.

190 Vgl. Art. 34d Abs. 3 S. 7, 8 BayPAG und § 31c Abs. 5 S. 5, 6 POG.

191 Vgl. BVerfG NJW 2008, 822, 832.

192 Art 34d Abs. 4 S. 2 BayPAG.

193 Vgl. Landesregierung, LT-Drs. 15/4879, S. 39; kritisch zu einer Sonderregelung für Gefahr im Verzug auch *Baum/ Schantz*, ZRP 2008, 137, 139.

194 Vgl. auch Bundesregierung, BT-Drs. 16/10121, S. 30.

3.2.8 Funkzellenabfrage (§ 31e POG)

Die Möglichkeit der Funkzellenabfrage (§ 31e POG) besteht in den Ländern Baden-Württemberg, Bayern, Hamburg und Schleswig-Holstein.[195] Einzigartig in Rheinland-Pfalz ist hierbei die Erwähnung in einer gesonderten Norm. Die anderen Bundesländer orientieren sich in ihrer Formulierung an § 100g Abs. 3 StPO. Die Regelungen aller Bundesländer sehen die Anordnung durch das Gericht[196] und die Möglichkeit der polizeilichen Anordnung in Fällen von Gefahr im Verzug[197] vor. Anstelle der Kennung eines TK-Anschlusses oder eines Endgeräts genügt insoweit „eine räumlich und zeitlich hinreichend bestimmte Bezeichnung der Telekommunikation“ (so die Formulierung in § 100g Abs. 2 S. 2 StPO). Im Umkehrschluss bedeutet dies: Wenn das Gesetz in bestimmten Fällen die Anforderungen an die gerichtliche Anordnung lockert – und damit eine formelle Bestimmung enthält – muss dies erst recht die Polizei materiell ermächtigen.

Gegenstand der Funkzellenabfrage sind in Bayern, Hamburg, Rheinland-Pfalz, Schleswig Holstein sowie in der StPO Verkehrsdaten[198], dagegen in Baden-Württemberg zusätzlich zu den Verkehrsdaten noch Daten der Telemediennutzung[199]. Die Begründung des Gesetzesentwurfs zu § 20m Abs. 3 S. 2 BKAG nennt für die Funkzellenabfrage nur Verkehrsdaten der Telekommunikation[200]. In der Kommentarliteratur[201] wird aber der gesamte Abs. 3 als nähere Regelung sowohl der Telekommunikationsdatenerhebung nach Abs. 1

---

195 Vgl. § 23a Abs. 2 S. 5 PolG BW; Art. 34c Abs. 3 S.2 Halbs. 2 BayPAG; § 10e Abs. 2 S. 2 PolDVG HA; § 185a Abs. 2 Nr.4, Abs.3 LVwG.

196 § 23a Abs. 2 S. 6, 7 iVm § 23 Abs. 3 S. 1 PolG BW; Art. 34c Abs. 3 S. 2 Halbs. 2, Abs. 1 S. 1 BayPAG iVm 34 Abs. 4 S. 1 BayPAG; § 10e Abs. 2 S. 2, Abs. 1 S. 1 PolDVG HA; § 31e Abs. 2 S. 1 iVm § 31 Abs. 4 S. 1 POG; § 185a Abs. 2 Nr. 4, Abs. 1 iVm § 186 Abs. 1 S. 1 LVwG S-H.

197 § 23a Abs. 2 S. 6, 7 iVm § 23 Abs. 3 S. 8 und 9 PolG BW; Art. 34c Abs. 3 S. 2 Halbs. 2, Abs. 1 S. 1 iVm Art. 34 Abs. 4 S. 1 Halbs. 1 BayPAG; § 10e Abs. 2 S. 2, Abs. 1 S. 2 PolDVG HA; § 31e Abs. 2 S. 2 Halbs. 1 iVm § 31 Abs. 5 S. 3 POG; § 185a Abs. 2 Nr. 4, Abs. 1 iVm § 186 Abs. 1 S. 2 LVwG S-H.

198 Art. 34c Abs. 3 S. 2 Halbs. 2 BayPAG; § 10e Abs. 2 PolDVG HA; § 31e Abs. 1 POG; § 185a Abs. 2 Nr. 4 LVwG S-H; § 100g Abs. 3 StPO.

199 § 23a Abs. 2 S. 6 PolG BW

200 BT-Drs. 16/10121, S. 33.

201 Vgl. *Schenke*, in: Schenke/ Graulich/ Ruthig, Sicherheitsrecht des Bundes, § 20m BKAG Rn. 24.

wie auch der Telemediennutzungsdaten nach Abs. 2 verstanden[202], so dass die Funkzellenabfrage auch letztere umfassen würde.

Dass die entsprechenden Normen nicht nur Verfahrens-, sondern auch Ermächtigungsgrundlagen darstellen, darüber besteht Einigkeit.[203]

3.2.9 Besondere Formen des Datenabgleichs (§ 38 POG, sog. Rasterfahndung)

3.2.9.1 Maßnahmevoraussetzungen

Besondere Formen des Datenabgleichs (sog. Rasterfahndungen) können angeordnet werden, „soweit dies zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person erforderlich ist“.[204] Vereinzelt sind auch weitere Rechtsgüter ge-

---

202 Vgl. *Schenke*, in: Schenke/ Graulich/ Ruthig, Sicherheitsrecht des Bundes, § 20m BKAG Rn. 24.

203 Vgl. *Schmidbauer*, in: Schmidbauer/ Steiner, BayPAG, Art. 34c Rn. 11; *Schmitt*, in: Meyer-Goßner/ Schmitt, StPO § 100g Rn.36.

204 In diesem Sinne Art. 44 Abs. 1 BayPAG: „soweit dies erforderlich ist zur Abwehr 1. einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder für Sachen, soweit eine gemeine Gefahr besteht, oder 2. einer schwerwiegenden Straftat, wenn konkrete Vorbereitungshandlungen für sich oder zusammen mit weiteren bestimmten Tatsachen die begründete Annahme rechtfertigen, dass eine solche begangen werden wird.“
§ 40 Abs. 1 S. 1 PolG BW: „soweit dies zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leben, Gesundheit oder Freiheit einer Person erforderlich ist.“
§ 47 Abs. 1 S. 1 ASOG Bln: „zur Abwehr einer durch Tatsachen belegten gegenwärtigen Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person […], soweit Tatsachen die Annahme rechtfertigen, dass das zur Abwehr der Gefahr erforderlich ist.“;
§ 46 Abs. 1 BbgPolG: „soweit dies zur Abwehr einer konkreten Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person erforderlich ist“;
§ 36i Abs. 1 S. 1 BremPolG: „soweit dies zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes, für Leib, Leben oder Freiheit einer Person oder zur Verhütung einer Straftat von erheblicher Bedeutung erforderlich ist.“;

§ 23 Abs. 1 PolDVG HA: „soweit dies zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person erforderlich ist";
§ 26 Abs. 1 S. 1 HSOG: „zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leben, Gesundheit oder Freiheit oder wenn gleichgewichtige Schäden für die Umwelt zu erwarten sind, [...], wenn dies zur Abwehr der Gefahr erforderlich ist.";
§ 44 Abs. 1 S. 1 SOG M-V: „zur Abwehr einer im einzelnen Falle bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person oder den Bestand oder die Sicherheit des Bundes oder eines Landes […] wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass dies zur Abwehr der Gefahr erforderlich ist.";
§ 45a Abs. 1 S. 1 Nds. SOG: „wenn die Gefahr auf andere Weise nicht abgewehrt werden kann, dass durch eine Straftat die Sicherheit oder der Bestand des Bundes oder eines Landes oder Leib, Leben oder Freiheit einer Person geschädigt werden oder dass schwere Schäden für die Umwelt oder für Sachen entstehen, deren Erhalt im öffentlichen Interesse geboten ist.";
§ 31 Abs. 1 S. 1 und 2 PolG NRW: „soweit dies zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person erforderlich ist (Rasterfahndung). Der Datenabgleich soll den Ausschluss von Personen bezwecken; er kann auch der Ermittlung eines Verdachts gegen Personen als mögliche Verursacher einer Gefahr sowie der Feststellung gefahrenverstärkender Eigenschaften dieser Personen dienen.";
§ 38 Abs. 1 POG: „soweit dies zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person erforderlich ist.";
§ 37 Abs. 1 SPolG: „zur Abwehr von Gefahren für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person […], soweit dies erforderlich ist.";
§ 47 Abs. 1 S. 1 SächsPolG: „soweit dies zur Abwehr einer konkreten Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person erforderlich ist";
§ 31 Abs. 1 SOG LSA: „wenn dies zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person erforderlich ist.";
§ 195a Abs. 1 LVwG „soweit dies erforderlich ist zur Abwehr einer erheblichen Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder zur Verhütung von Straftaten erheblicher Bedeutung, bei denen Schäden für Leben, Leib und Freiheit oder gleichgewichtige Schäden für die Umwelt zu erwarten sind und die Verhütung des Schadens auf andere Weise nicht möglich ist.";
§ 44 Abs. 1 ThürPAG: „wenn dies zur Abwehr einer Gefahr für den Bestand oder die Sicherheit der Bundesrepublik Deutschland oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder zur Abwehr einer gemeinen Gefahr für Sachen, erforderlich ist.".

schützt. So ist beispielsweise gemäß § 26 Abs. 1 S. 1 HSOG eine Rasterfahndung auch zulässig, „wenn gleichgewichtige Schäden für die Umwelt zu erwarten sind“.

Enger wird in Bremen und Niedersachsen der Charakter als ultima ratio im Gesetz ausdrücklich festgeschrieben.[205]

3.2.9.2 Richtervorbehalt

Die Rasterfahndung setzt in sieben Bundesländern eine richterliche Entscheidung voraus,[206] wobei die Maßnahme bei Gefahr im Verzug gemäß § 38 Abs. 3 S. 5 POG und gemäß § 47 Abs. 3 S. 2 SächsPolG auch (vorläufig) durch die Behörde angeordnet werden kann.

Zuständig bei Richtervorbehalt ist das Amtsgericht, in dessen Bezirk die Polizeidienststelle ihren Sitz hat[207], bzw. zentral das Amtsgericht Tiergarten[208].

Ein Richtervorbehalt war für Baden-Württemberg, Bremen, Hamburg, Hessen und Mecklenburg-Vorpommern, Niedersachsen, das Saarland (vgl. § 37 Abs. 4 S. 1 SPolG), Sachsen-Anhalt (vgl. § 31 Abs. 4 S. 1 SOG LSA) und Thüringen (vgl. § 44 Abs. 4 ThürPAG) nicht ersichtlich. In Ländern ohne Richtervorbehalt sind teilweise höhere Behörden eingebunden. So darf die Rasterfahndung gemäß § 44 Abs. 4 S. 1 SOG M-V nur vom Innenministerium bzw. gemäß § 23 Abs. 4 S. 1 PolDVG HA vom Präses oder Staatsrat der für die Polizei zuständigen Fachbehörde angeordnet werden, bzw. sie bedarf gemäß § 40 Abs. 3 S. 1 PolG BW, § 36i Abs. 3 S. 1 BremPolG, § 45a Abs. 2 S. 1 Nds. SOG oder § 31 Abs. 4 S. 1 SOG LSA der Zustimmung des Senators bzw. Ministeriums

---

205 § 36i Abs. 1 S. 2 BremPolG: „Die Maßnahme darf nur angeordnet werden, wenn die Abwehr der Gefahr auf andere Weise weniger erfolgversprechend oder nicht möglich wäre.“;
§ 45a Abs. 1 S. 1 Nds. SOG „wenn die Gefahr auf andere Weise nicht abgewehrt werden kann“;
§ 195a Abs. 1 LVwG: “soweit … die Verhütung des Schadens auf andere Weise nicht möglich ist”.

206 Art. 44 Abs. 3 S. 1 BayPAG; § 47 Abs. 4 S. 1 ASOG Bln; § 46 Abs. 4 S. 1 BbgPolG; § 31 Abs. 4 S. 1 PolG NRW; § 38 Abs. 3 S. 1 POG; § 47 Abs. 3 S. 1 SächsPolG; § 195a Abs. 2 S. 1 LVwG.

207 So Art. 44 Abs. 3 S. 2 BayPAG; § 38 Abs. 3 S. 2 POG; § 46 Abs. 4 S. 2 BbgPolG; § 31 Abs. 4 S. 2 PolG NRW; § 38 Abs. 3 S. 2 POG; § 195a Abs. 2 S. 2 LVwG: Sitz des Landeskriminalamtes.

208 § 47 Abs. 4 S. 2 ASOG Bln.

für Inneres oder gemäß § 26 Abs. 4 HSOG der Zustimmung des Landespolizeipräsidiums.

3.2.9.3 Beteiligung des Landesdatenschutzbeauftragten

Über die Rasterfahndung ist in den meisten Bundesländern der Landesbeauftragte für Datenschutz zu unterrichten[209], was zumeist unverzüglich[210], unverzüglich nach Abschluss[211] oder fortlaufend[212] zu erfolgen hat. Demgegenüber war eine Benachrichtigungspflicht nicht ersichtlich in Brandenburg und Nordrhein-Westfalen.

3.2.9.4 Reichweite der Maßnahme

In allen Bundesländern kann von öffentlichen und nichtöffentlichen Stellen die Übermittlung von personenbezogenen Daten bestimmter Personengruppen aus Dateien zum Zweck des Abgleichs mit anderen Datenbeständen verlangt werden.[213] Das Übermittlungsersuchen ist auf „Namen, Anschriften, Tag und Ort der Geburt“ und andere für den Einzelfall benötigte Daten zu beschränken[214]. Darüber hinaus verlangt § 47 Abs. 2 S. 1 i.V.m. § 18 Abs. 3 SächsPolG die Angabe von früheren Namen sowie Staatsangehörigkeiten.

---

209 § 44 Abs. 4 S. 2 SOG M-V; § 37 Abs. 4 S. 2 SPolG.

210 Art. 44 Abs. 3 S. 6 BayPAG, § 40 Abs. 3 S. 2 PolG BW; § 36i Abs. 3 S. 2 BremPolG; § 26 Abs. 4 S. 2 HSOG; § 45a Abs. 2 S. 2 Nds. SOG; § 38 Abs. 3 S. 3 POG; § 47 Abs. 4 SächsPolG; § 31 Abs. 4 S. 2 SOG LSA; § 195a Abs. 6 LVwG: über den Beginn und den Abschluss; § 44 Abs. 4 S. 2 ThürPAG.

211 § 23 Abs. 4 S. 2 PolDVG HA.

212 § 47 Abs. 4 S. 11 ASOG Bln.

213 In diesem Sinne: § 40 Abs. 1 PolG BW; Art. 44 Abs. 1 BayPAG, § 40 Abs. 3 S. 2 PolG BW, § 47 Abs. 1 S. 1 ASOG Bln; § 46 Abs. 1 BbgPolG; § 36i Abs. 1 S. 1 BremPolG; § 23 Abs. 1 PolDVG HA, § 26 Abs. 1 S. 1 HSOG; § 44 Abs. 1 S. 1 SOG M-V; § 45a Abs. 1 S. 1 Nds. SOG; § 31 Abs. 1 S. 1 PolG NRW; § 38 Abs. 1 POG; § 37 Abs. 1 S. 1 SPolG; § 47 Abs. 1 S. 1 SächsPolG; § 31 Abs. 1 SOG LSA; § 195a Abs. 1 LVwG; § 44 Abs. 1 ThürPAG.

214 In diesem Sinne: § 40 Abs. 2 S. 1 PolG BW; Art. 44 Abs. 2 S. 1 BayPAG, § 47 Abs. 2 S. 1 ASOG Bln; § 46 Abs. 2 S. 1 Halbs. 1 BbgPolG; § 36i Abs. 2 S. 2 BremPolG; § 23 Abs. 2 S. 2 PolDVG HA, § 26 Abs. 2 S. 1 HSOG; § 44 Abs. 2 S. 1 SOG M-V, § 45a Abs. 1 S. 1 Nds. SOG; § 31 Abs. 2 S. 1 PolG NRW; § 38 Abs. 2 S. 1 POG; § 37 Abs. 2 S. 1 SPolG; § 47 Abs. 2 S. 1 SächsPolG; § 31 Abs. 2 S. 1 SOG LSA; § 195a Abs. 3 S. 1 LVwG; § 44 Abs. 2 S. 1 ThürPAG.

3.2.10 Schutz des Kernbereichs privater Lebensgestaltung (§ 39a POG)

Ein an der Rechtsprechung des BVerfG[215] orientierter Schutz des Kernbereichs privater Lebensgestaltung ist mittlerweile in allen Landesregelungen enthalten.[216] Die Regelungen in den Ländern stimmen weitgehend überein: Die Maßnahme darf nicht angeordnet werden bzw. muss unterbrochen werden, sobald der Kernbereich berührt ist. Es entsteht ein Verwertungsverbot, die Daten sind unverzüglich zu löschen und die Tatsache der Datenerhebung ist zu dokumentieren. Die Maßnahme darf fortgesetzt werden, wenn die Voraussetzungen der Anordnung wieder erfüllt sind.

Einige Abweichungen sind allerdings zu beachten: In Bremen und Hessen fehlt es an der Regelung, dass Maßnahmen, die den Kernbereich berühren, zu unterbrechen sind. In Hessen ergibt sich dies jedoch aus der Formulierung, wonach die „Maßnahme unzulässig" ist.[217] Dieselbe Formulierung findet sich in § 100a Abs. 4 S. 1 StPO. In Bremen findet sich nichts derartiges, was nicht den Vorgaben des BVerfG entspricht.[218]

In Thüringen fehlt es an einer Regelung, die dazu verpflichtet, die Tatsache der Datenerhebung aus dem Kernbereich privater Lebensgestaltung zu dokumentieren. Während in den meisten Ländern und im Bund geregelt ist, unter welchen Voraussetzungen die unterbrochenen Maßnahmen fortgeführt werden dürfen,[219] fehlen in Bayern, Bremen, Niedersachsen, Saarland und Sach-

---

215 Siehe dazu BVerfG, Urt. v. 3.3.2004 – 1 BvR 2378/98.

216 Vgl. § 23 Abs. 2 und 5 PolG BW; Art. 34 Abs. 2, Abs. 5 S. 3 Nr. 3, Abs. 7, Art. 34a Abs. 1 S. 4, Art. 34c Abs. 4 S. 3 Nr. 3, Abs. 6 S. 1, Art 34d Abs. 1 S. 5 und 6, Abs. 4 S. 1 Nr. 1, Absatz 5 S. 3 Nr. 3 BayPAG; § 25 Abs. 4a ASOG Bln; § 29 Abs. 6, § 33a Abs. 3, 5, § 33b Abs. 2 S. 2 BbgPolG; § 33 Abs. 4 BremPolG; § 10 Abs. 3 S. 2 ff, § 10a Abs. 5 S. 4, Abs. 7 S. 6, § 10e Abs. 3 S. 5, Abs. 5 S. 6 PolDVG HA; § 15 Abs. 4 S. 4 und 5, § 27 Abs. 2, 3, 6 S. 1 Nr. 2 HSOG; § 34a Abs. 8 S. 4, § 34b Abs. 2 und 3 SOG M-V; § 33a Abs. 3, § 35 Abs. 2, § 35a Abs. 2, 3, § 36 Abs. 4 Nds. SOG; § 16, § 18 Abs. 3 und 4 PolG NRW; § 39a POG, § 28d SPolG, § 41 Abs. 6und 7 SächsPolG; § 17 Abs. 4a-4c, § 17b Abs. 5 SOG LSA; § 186a Abs. 1-3 LVwG; § 34a Abs. 1 S. 3, Abs. 4, § 35 Abs. 2, Abs. 6 und 7, § 36 Abs. 2 ThürPAG.

217 Vgl. § 15 Abs. 4 S. 4 HSOG; Meixner/ Fredrich, HSOG, § 15 Rn. 11.

218 Vgl. BVerfG, Urt. v. 3.3.2004 – 1 BvR 2378/98, Rn. 169.

219 Vgl. § 23 Abs. 5 S. 2 PolG BW; § 25 Abs. 4a S. 5 ASOG Bln; § 33a Abs. 5 S. 3 BbgPolG; § 10 Abs. 3 S. 5 PolDVG HA; § 34b Abs. 3 S. 4 SOG M-V; § 16 Abs. 2 S. 2 PolG NRW; § 18 Abs. 4 S. 3 PolG NRW; § 17 Abs. 4b S. 3 SOG LSA; § 186a Abs. 2 S. 3 LVwG; § 35 Abs. 6 S. 3, § 34b Abs. 1 ThürPAG; § 20h Abs. 5 S. 5 BKAG; § 100c Abs. 5 S. 4 StPO.

sen derartige Bestimmungen. Hat die Polizei Zweifel, ob der Kernbereich berührt ist, darf in sechs Bundesländern nur eine automatische Aufzeichnung fortgesetzt werden[220], über deren Verwertbarkeit zumeist unmittelbar ein Richter zu entscheiden hat[221]. In Nordrhein-Westfalen besteht diese Einschränkung nur im Fall der Wohnraumüberwachung.[222] In Sachsen-Anhalt kann eine automatische Aufzeichnung dagegen fortgesetzt werden, auch wenn Zweifel über den berührten Kernbereich bestehen.[223]

Einzigartig ist die Stellung des Gerichts in Rheinland-Pfalz: Es ist neben der Überprüfung auch zur Sachleitung berechtigt und verpflichtet (vgl. § 39a Abs. 4 POG). Nur für den verdeckten Eingriff in informationstechnische Systeme sieht § 20k Abs. 7 S. 3 BKAG ebenfalls die Sachleitung des anordnenden Gerichts vor. Einige Länder beschränken sich auf die Überprüfung der Verwertung durch das Gericht,[224] während die übrigen Länder insoweit keine Bestimmungen treffen (Baden-Württemberg, Brandenburg, Bremen, Niedersachsen, Saarland, Schleswig-Holstein).

Eine Besonderheit in Rheinland-Pfalz, im Saarland und im BKAG ist es, dass sowohl zwei Bedienstete der Polizeibehörde als auch der behördliche Datenschutzbeauftragte dazu verpflichtet sind, kernbereichsrelevante Daten durchzusichten.[225] In Nordrhein-Westfalen tritt eine „Leitungsperson“ an Stelle der Bediensteten.[226]

---

220 Vgl. § 10 Abs. 3 S. 3 PolDVG HA; § 15 Abs. 4 S. 5 HSOG, § 18 Abs. 4 S. 2 PolG NRW; § 39a Abs. 5 S. 2 POG; § 35 Abs. 6 S. 4 ThürPAG; in Bayern ergibt sich dies aus einer Gesamtbetrachtung der Art. 34 Abs. 1 S. 2 Nr.1, Abs. 2 S. 1 BayPAG.

221 So § 10 Abs. 3 S. 4 PolDVG HA; § 15 Abs. 5 S. 10 HSOG; § 34 Abs. 3 S. 5 ThürPAG; § 35 Abs. 6 S. 5 ThürPAG.

222 Vgl. § 18 Abs. 4 S. 2 PolG NRW.

223 Vgl. § 17 Abs. 4b S. 2 SOG LSA.

224 Vgl. Art. 34 Abs. 5 S. 4 BayPAG; § 25 Abs. 5 S. 13 ASOG Bln; § 10 Abs. 3 S. 4 PolDVG HA; § 15 Abs. 5 S. 1 HSOG; § 34b Abs. 6 S. 3 SOG M-V; § 16 Abs. 3 S. 2; § 16 Abs. 3 S. 4 PolG NRW; § 18 Abs. 4 S. 4 PolG NRW; § 28d Abs. 3 S. 2 SPolG („Im Zweifelsfall“); § 41 Abs. 7 S. 4 SächsPolG; § 17 Abs. 5a SOG LSA; § 35 Abs. 6 S. 5 ThürPAG.

225 Vgl. § 39a Abs. 4 S. 3 POG; § 28d Abs. 3 S. 1 SPolG; § 20k Abs. 7 S. 3 BKAG (vgl. dazu, dass dies keine hinreichend unabhängige Kontrolle ist, BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09, Rn. 224, 225).

226 Vgl. § 16 Abs. 3 S. 1 PolG NRW.

Der Umfang des Kernbereichsschutzes ist unterschiedlich. In einigen Ländern sowie im Bundesrecht betrifft er nur die Wohnraumüberwachung,[227] in den übrigen Ländern allgemein den Einsatz verdeckter Mittel.

In Bayern und Hamburg werden für die Wohnraumüberwachung Fallkonstellationen aufgeführt, in denen der Kernbereich tangiert sein könnte.[228] Dazu gehört es, wenn sich die betroffene Person allein oder mit engsten Familienangehörigen in der Wohnung aufhält, Gespräche geführt werden, die einen Bezug zu der Gefahr haben, die zu der Maßnahme ermächtigt oder sich die Maßnahmen auch gegen Familienangehörige und Vertraute richtet. Nach der Rechtsprechung des BVerfG ist es allerdings nicht erforderlich, derartige Fallgruppen zu normieren.[229]

3.2.11 Schutz von Berufsgeheimnisträgern (§ 39b POG)

In den meisten Bundesländern ist ein dem § 39b POG vergleichbarer Schutz Zeugnisverweigerungsberechtigter vorgesehen.[230] Einige Länder beschränken sich darauf, die Datenerhebung für unzulässig zu erklären.[231] In Rheinland-Pfalz und anderen Ländern wird teilweise darüber hinaus formuliert, dass die Daten unverzüglich zu löschen sind, Erkenntnisse nicht verwertet werden dürfen und die Tatsache der Datenerhebung zu dokumentieren ist.[232] In Nordrhein-Westfalen und im Saarland wird auf die Bestimmungen zum Schutz des

---

227 Vgl. § 23 Abs. 2, 5 PolG BW; § 25 Abs. 4a ASOG BlnBbgPolG, § 20h Abs. 5 BKAG, § 100a, 100c StPO; § 33a Abs. 3, 5 BbgPolG (Wohnraumüberwachung); § 33b Abs. 2 BbgPolG (Telekommunikationsüberwachung); § 34a Abs. 8 S. 5 SOG M-V (Telekommunikationsüberwachung); § 34b Abs. 2, 3 SOG M-V (Wohnraumüberwachung).

228 Vgl. Art. 34 Abs. 1 S. 2 BayPAG, § 10a Abs. 1 S. 2 PolDVG HA.

229 Vgl. BVerfG NJW 2007, 2753, 2754.

230 Vgl. § 9a PolG BW; Art. 34 Abs. 1, 3, 5, 8 BayPAG; § 25 Abs. 4a S. 10 ASOG Bln; § 33a Abs. 2 S. 6 BbgPolG; § 33b Abs. 2 S. 3 BbgPolG; § 33 Abs. 9 BremPolG; § 10 Abs. 3 PolDVG HA; § 33 Abs. 6 SOG M-V; § 30 Abs. 7 Nds. SOG; § 16, 18 Abs. 3 PolG NRW; § 28a Abs. 2 SPolG; § 41 Abs. 6 S. 1 Nr. 2 SächsPolG; § 17 Abs. 4d SOG LSA; § 186a Abs. 4 LVwG; § 34a Abs. 1, S. 4, Abs. 4 ThürPAG, § 34b Abs. 1 S. 3, Abs. 2 ThürPAG.

231 Vgl. Art. 34 BayPAG; § 25 Abs. 4a S. 10 ASOG Bln; § 33 Abs. 9 BremPolG; § 10 Abs. 3 S. 1 PolDVG HA; § 33 Abs. 6 SOG M-V; § 30 Abs. 7 S. 1 Nds. SOG.

232 Vgl. § 9a Abs. 1 PolG BW; § 33b Abs. 2, 10 BbgPolG; § 39b POG; § 41 Abs. 6, 7 SächsPolG; § 17 Abs. 4d S. 2 SOG LSA; § 186a Abs. 4 S. 2 LVwG; § 34a Abs. 1 S. 4, Abs. 4 ThürPAG.

Kernbereichs verwiesen.[233] Hessen kennt keine Beschränkung der Datenerhebung zum Schutz zeugnisverweigerungsberechtigter Berufsgeheimnisträger. § 21 Abs. 2 HSOG begrenzt lediglich die Datenübermittlung. Dadurch, dass Rheinland-Pfalz die Berufsgeheimnisträger nach §§ 53, 53a StPO generell erfasst und nicht zwischen bestimmten Berufsgruppen unterscheidet, geht es über die Anforderungen des BVerfG[234] hinaus. Dies führt zu einem rechtlichen Problem (→ Kapitel 3.3.11.1, S. 142 f.).

Während in Rheinland-Pfalz und anderen Bundesländern das Berufsgeheimnis allgemein für die Fälle der Datenerhebung geschützt ist,[235] beschränken andere Länder den Schutz auf die Wohnraumüberwachung.[236]

Die meisten Polizeigesetze der Länder verweisen auf die Vorschriften der §§ 53, 53a StPO, der Schutz in Bremen erstreckt sich nur auf die Fälle des § 53 StPO.[237] In Hessen gilt der Schutz nur für die Datenübermittlung.

In der StPO ist bei Maßnahmen gegen zeugnisverweigerungsberechtigte Personen zwischen zwei verschiedenen „Schutzstufen“ zu unterscheiden, wobei zusätzlich zwischen Wohnraumüberwachung und sonstigen Maßnahmen differenziert werden kann:

Hinsichtlich der Wohnraumüberwachung gemäß § 100c Abs. 6 StPO gilt ein absoluter Schutz für alle in § 53 StPO aufgezählte Berufsgruppen, also ein Erhebungs- und Verwertungsverbot. Für die Fälle der §§ 52 und 53a StPO gilt ein relativer Schutz: Ein Verwertungsverbot kann sich nach Abwägung im Einzelfall ergeben.[238]

---

233 Vgl. § 16 Abs. 5, 18 Abs. 3 PolG NRW und § 28d Abs. 1 Halbs. 2 SPolG.

234 Vgl. BVerfG, Urteil vom 03.03.2004 – 1 BvR 2378/98, Rn. 147.

235 Vgl. § 9a PolG BW; § 33a Abs. 2 S. 6 BbgPolG (Wohnraumüberwachung); § 33b Abs. 2 S. 3 BbgPolG (Telekommunikatonsüberwachung, Verkehrs- und Nutzungsdatenauskunft); § 33 Abs. 9 BremPolG; § 10 Abs. 3 S. 1 PolDVG HA; § 33 Abs. 6 SOG M-V; § 30 Abs. 7 Nds. SOG, § 16 Abs. 5 PolG NRW; § 18 Abs. 3 PolG NRW (Datenerhebung in und aus Wohnungen); § 39b PolG; § 28d SPolG; § 17 Abs. 4d SOG LSA; § 186a Abs. 4 LVwG; § 34a Abs. 1 S. 4, Abs. 4 ThürPAG (Telekommunikationsüberwachung), § 34b Abs.1 S. 3, Abs. 2 ThürPAG (Verkehrs-, Nutzungsdatenerhebung), § 35 Abs. 2, Abs. 6 ThürPAG (Wohnraumüberwachung), § 36 Abs. 2 ThürPAG.

236 Vgl. Art. 34 BayPAG; § 25 Abs. 4a S. 10 ASOG Bln; § 41 Abs. 6 SächsPolG.

237 Vgl. § 33 Abs. 9 BremPolG.

238 Der einschlägige § 100c Abs. 6 StPO wurde vom BVerfG für verfassungskonform erachtet, NJW 2007, 2753, 2756.

Hinsichtlich sonstiger Maßnahmen gemäß § 160a StPO ist innerhalb des § 53 StPO zwischen einem absoluten Schutz für bestimmte Berufsgruppen und einem relativen Schutz im Rahmen der Verhältnismäßigkeitsprüfung zu differenzieren.

Eine dem § 160a StPO ähnliche Differenzierung zwischen absolutem und relativem Schutz von Berufsgruppen haben die Länder Baden-Württemberg, Bayern sowie Mecklenburg-Vorpommern für das Beichtgeheimnis. [239] In Thüringen ist der Schutz bei Wohnraumüberwachungen absolut, im Übrigen relativ.[240] Die meisten Länder differenzieren nicht zwischen einzelnen Berufsgruppen. Viele sehen insoweit einen absoluten Schutz vor,[241] während Niedersachsen und Schleswig-Holstein Berufsgruppen nur relativ schützen: Die Formulierung, dass die Maßnahme ausnahmsweise zulässig ist, wenn es zur Abwehr einer unmittelbar bevorstehenden Gefahr bzw. gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist,[242] eröffnet eine Verhältnismäßigkeitsprüfung. Ähnliche Regelungen finden sich auch für die ausnahmsweise zulässige Verwendung erhobener Daten[243].

Teilweise wird die Erhebung erlaubt, soweit ein unmittelbarer Bezug zwischen den erfassten Inhalten und der abzuwehrenden Gefahr besteht.[244] Hat die zeugnisverweigerungsberechtigte Person die Gefahr verursacht oder ist sie dafür verantwortlich, so entfällt der Schutz der Berufsgeheimnisträger in Rheinland-Pfalz und einigen anderen Ländern.[245] Jemand verursacht die Gefahr, wenn er Handlungs- oder Zustandsstörer ist.[246] Bedenken gegen die Bestimmtheit werden nicht erhoben.

---

239 Vgl. § 9a Abs. 2 S. 2 PolG BW; Art. 34 Abs. 1 S. 2, Abs. 5 S. 3 BayPAG; § 33 Abs. 6 S. 2 SOG M-V.

240 Vgl. § 5 Abs. 3, § 35 Abs. 2 ThürPAG.

241 Vgl. § 25 Abs. 4a S. 10 ASOG Bln; § 33a Abs. 2 S. 5; § 33b Abs. 2 S. 3 BbgPolG; § 33 Abs. 9 BremPolG; § 10 Abs. 3 S. 1 PolDVG HA; § 33 Abs. 6 SOG M-V; § 16 Abs. 5, § 18 Abs. 3 PolG NRW; § 28d Abs. 1 SPolG; § 41 Abs. 6 SächsPolG; § 17 Abs. 4d SOG LSA.

242 § 30 Abs. 7 S. 1 Nds. SOG und § 186a Abs. 4 S. 1 LVwG.

243 Vgl. Art. 34 Abs. 5 S. 3 Halb. 2 und 4 BayPAG; § 33b Abs. 10 S. 1 und 2 BbgPolG; § 36 Abs. 2 S. 2 und 3 ThürPAG.

244 Vgl. § 34a Abs. 4 S. 1 Nr. 3 ThürPAG und § 35 Abs. 6 S. 1 Nr. 3 ThürPAG

245 Vgl. § 9a Abs. 4 PolG BW; § 39b Abs. 2 POG; § 33 Abs. 6 SOG M-V; ähnlich Art. 34 Abs. 1 S. 2 Nr. 3 BayPAG, Art. 34a Abs.1 S. 3 BayPAG; Art .34d Abs. 1 S. 4; § 33b Abs. 2 S. 2 BbgPolG, die eine gegen den Berufsträger gerichtete Datenerhebung erlauben.

246 Vgl. *Stephan/ Deger*, PolG BW, § 9a Rn. 7; *Berner/ Köhler/ Käß*, BayPAG, Art. 34 Rn. 8; *Ebert/ Seel*, ThürPAG, § 5 Rn. 43.

3.2.12 Pflichten zur Benachrichtigung der Betroffenen (§ 40 Abs. 5, 6 POG)

3.2.12.1 Maßnahme mit Benachrichtigungspflichten

Die Betroffenen der zu evaluierenden, verdeckten Datenerhebungsmaßnahmen sind nach den Regelungen in 13 Bundesländern[247] generell zu unterrichten. Außerdem haben fünf Bundesländer speziell eine Benachrichtigungspflicht nach einer Wohnraumüberwachung[248] geregelt. Vier dieser fünf Länder haben auch eine Benachrichtigungspflicht nach einer Rasterfahndung[249], während in Mecklenburg-Vorpommern eine entsprechende Regelung nicht ersichtlich war. Angesichts dieser Heterogenität ist hinsichtlich des Vergleichs eine Beschränkung auf die Benachrichtigungspflichten nach einer verdeckten Wohnraumüberwachung angezeigt.

3.2.12.2 Voraussetzungen für die Benachrichtigungspflicht

Personen, gegen die sich eine verdeckte Datenerhebung richtet, sind in neun Bundesländern grundsätzlich zu unterrichten.[250] Prinzipiell ebenso sind sonstige betroffene Personen in sieben Bundesländern zu benachrichtigen.[251] Bei letzteren wird in Berlin und Mecklenburg-Vorpommern weiter zwischen anderen Personen, wenn die Maßnahme zur vorbeugenden Bekämpfung von Straftaten unerlässlich ist, und Personen, die sich als Gast oder sonst zufällig

---

247 § 25 Abs. 7 und 7a ASOG Bln; § 29 Abs. 7 BbgPolG; § 33 Abs. 5 BremPolG; § 10a Abs. 6, § 23 Abs.5 PolDVG HA; § 29 Abs. 6 HSOG; § 30 Abs. 4-6 Nds. SOG; § 17 Abs. 5-6 PolG NRW; § 40 Abs. 5-6 POG; § 28 Abs. 5 SPolG; § 17 Abs. 7 SOG LSA; § 186 Abs. 4 und 5 LVwG; § 36 Abs. 3 ThürPAG.

248 Art. 34 Abs. 6 BayPAG; § 23 Abs. 6 PolG BW; § 10a Abs. 6 PolDVG HA; § 34b Abs. 8 SOG M-V; § 41 Abs. 8 SächsPolG.

249 Art. 44 Abs. 5 BayPAG; § 40 Abs. 5 PolG BW; § 23 Abs. 5 PolDVG HA; § 47 Abs. 5 SächsPolG.

250 § 40 Abs. 5 S. 1 POG; § 25 Abs. 7 S. 1 ASOG Bln; § 33 Abs. 5 S. 1 BremPolG; § 10a Abs. 6 S. 1 PolDVG HA; § 29 Abs. 6 S. 1 und 2 HSOG; § 34b Abs. 8 S. 1, 6 und 7 SOG M-V; § 17 Abs. 7 S. 1 SOG LSA; § 186 Abs. 4 S. 1 LVwG; § 34 Abs. 9 S. 1 ThürPAG.

251 § 40 Abs. 5 S. 2 POG; § 25 Abs. 7 S. 1 (und 3) ASOG Bln; § 33 Abs. 5 S. 1 BremPolG; § 10a Abs. 6 S. 1, § 23 Abs. 5 PolDVG HA; § 29 Abs. 6 S. 1 und 2 HSOG; § 34b Abs. 8 S. 1, 5, 6 SOG M-V; § 186 Abs. 4 S. 1, 2 LVwG; § 36 Abs. 3 1 ThürPAG.

in der überwachten Wohnung aufgehalten haben, differenziert.[252] Die übrigen acht Bundesländer differenzieren hinsichtlich der Art der Betroffenheit nicht.[253]

Die Benachrichtigungspflicht setzt in allen Bundesländern voraus, dass die Unterrichtung ohne Gefährdung des Zwecks der Maßnahme geschehen kann.[254] Weitere Hinderungsgründe können sich aus der Gefahr für die bei dem polizeilichen Einsatz eingesetzten Personen[255], für die zur Datenerhebung berechtigenden Rechtsgüter[256] oder für bedeutende Vermögenswerte[257] ergeben. Eine Unterrichtung kann auch unterbleiben, wenn „überwiegende schutzwürdige Belange eines Betroffenen entgegenstehen“[258]. Zudem kann gemäß § 36 Abs. 3 S. 3 ThürPAG die Unterrichtung einer unbeteiligten Person unterbleiben, „wenn diese von der Maßnahme nur unerheblich betroffen war und anzunehmen ist, dass sie kein Interesse an einer Benachrichtigung hat.“

252 Vgl. § 25 Abs. 7 S. 2, 3 ASOG Bln und § 34b Abs. 8 S. 6 SOG M-V.

253 Art. 34 Abs. 6 S. 1 BayPAG; § 23 Abs. 6 S. 1 PolG BW; § 25 Abs. 7 S. 1 ASOG Bln; § 29 Abs. 7 BbgPolG; § 30 Abs. 4 S. 1 Nds. SOG; § 17 Abs. 5 S. 1 PolG NRW; § 28 Abs. 5 S. 1 SPolG; § 41 Abs. 8 S. 1 SächsPolG.

254 In diesem Sinne: Art. 34 Abs. 6 S. 1 BayPAG; § 23 Abs. 6 S. 1 PolG BW; § 25 Abs. 7 S. 4 ASOG Bln; § 29 Abs. 7 S. 1 BbgPolG; § 33 Abs. 5 S. 1 BremPolG; § 10a Abs. 6 S. 1 PolDVG HA; § 29 Abs. 6 S. 4 HSOG; § 34b Abs. 8 S. 1 SOG M-V; § 30 Abs. 4 S. 3 Nds. SOG; § 17 Abs. 5 S. 1 PolG NRW; § 40 Abs. 5 S. 4 POG; § 28 Abs. 5 S. 1 SPolG; § 41 Abs. 8 S. 1 SächsPolG; § 17 Abs. 7 S. 1 SOG LSA; § 186 Abs. 4 S. 4 LVwG; § 36 Abs. 4 S. 1 ThürPAG.

255 In diesem Sinne: Art. 34 Abs. 6 S. 1 BayPAG; § 23 Abs. 6 S. 1 PolG BW; § 36 Abs. 4 S. 2 ThürPAG.

256 In diesem Sinne: Art. 34 Abs. 6 S. 1 BayPAG; § 25 Abs. 7 S. 4 ASOG Bln; § 29 Abs. 6 S. 4 HSOG; § 30 Abs. 5 S. 1 Nr. 2 Nds. SOG; § 17 Abs. 5 S. 1, 5 PolG NRW; § 40 Abs. 5 S. 4 POG, § 41 Abs. 8 S. 1 SächsPolG; § 186 Abs. 4 S. 4 LVwG; § 36 Abs. 4 S. 2 ThürPAG.

257 § 25 Abs. 7 S. 4 ASOG Bln; § 40 Abs. 5 S. 4 POG; § 186 Abs. 4 S. 4 LVwG.

258 § 33 Abs. 5 S. 4 Nr. 2 BremPolG, in diesem Sinne: § 30 Abs. 5 S. 1 Nr. 3 Nds. SOG; § 17 Abs. 5 S. 5 PolG NRW; § 28 Abs. 5 S. 2 SPolG; § 186 Abs. 4 S. 2 LVwG (bei unvermeidbar betroffenen Dritten); § 36 Abs. 3 S. 2 ThürPAG.

Sollte ein strafrechtliches Ermittlungsverfahren eingeleitet worden sein, führt das per se zum Wegfall der Benachrichtigungspflicht in vier Bundesländern[259], während in neun Bundesländern[260] insoweit eine Abstimmung mit der Staatsanwaltschaft stattzufinden hat. Eine Regelung im Zusammenhang mit Ermittlungsverfahren war nicht ersichtlich in § 33 Abs. 5 BbgPolG, § 33 Abs. 5 BremPolG und § 10a Abs. 6 PolDVG HA.

Eine Unterrichtung kann in einigen Bundesländern auch unterbleiben, wenn keine Aufzeichnung mit personenbezogenen Daten erstellt[261] oder diese unverzüglich nach Beendigung der Maßnahme vernichtet[262] wurden. Ein weiterer Grund für die Nichtbenachrichtigung kann in neun Bundesländern darin liegen, dass eine Benachrichtigung eine weitere Datenerhebung voraussetzt.[263] Hinzukommen muss zumeist, dass dies „im Interesse der betroffenen Person nicht geboten erscheint“[264] oder „die Identität oder der Aufenthaltsort eines Betroffenen nur mit unverhältnismäßigem Aufwand ermittelt werden kann“[265]. Ähnliches bestimmt § 34 Abs. 9 S. 2 ThürPAG: „Nachforschungen zur Feststellung der Identität einer zu benachrichtigenden Person sind nur vorzunehmen, wenn dies unter Berücksichtigung der Eingriffsintensität der Maß-

259 § 40 Abs. 6 Nr. 1 POG; § 28 Abs. 5 S. 3 SPolG; § 17 Abs. 7 S. 2 Nr. 1 SOG LSA; in diesem Sinne wohl auch: § 30 Abs. 5 S. 1 Nr. 1 Nds. SOG („solange Zwecke der Verfolgung einer Straftat entgegenstehen“).

260 In diesem Sinne Art. 34 Abs. 6 S. 2 BayPAG; § 23 Abs. 6 S. 2 PolG BW; § 25 Abs. 7 S. 8 ASOG Bln; § 29 Abs. 7 HSOG; § 34b Abs. 8 S. 4 SOG M-V; § 17 Abs. 5 S. 4 PolG NRW; § 41 Abs. 8 S. 2 SächsPolG; § 186 Abs. 5 S. 1 LVwG; § 36 Abs. 4 S. 3 ThürPAG.

261 § 34b Abs. 8 S. 6 SOG M-V (bei Personen, die sich als Gast oder sonst zufällig in der überwachten Wohnung aufgehalten haben („wenn die Überwachung keine verwertbaren Ergebnisse erbracht hat“); § 40 Abs. 6 Nr. 3 Alt. 1 POG.

262 § 40 Abs. 6 Nr. 3 Alt. 2 POG und § 17 Abs. 7 S. 2 Nr. 4 SOG LSA.

263 § 17 Abs. 7 S. 2 Nr. 3 SOG LSA.

264 § 40 Abs. 6 Nr. 2 POG, in diesem Sinne auch: § 29 Abs. 6 S. 3 HSOG: „im überwiegenden Interesse der Person liegt, gegen die sich die Maßnahme gerichtet hat“; § 34b Abs. 8 S. 5 SOG M-V: „überwiegende schutzwürdige Belange anderer Betroffener“ (außer bei Personen, gegen die sich die Maßnahme richtete).

265 § 33 Abs. 5 S. 4 Nr. 3 BremPolG, in diesem Sinne für erforderliche Datenerhebungen, die „in unverhältnismäßiger Weise“ oder „mit unverhältnismäßigen Ermittlungen“ erfolgen würden auch: § 29 Abs. 7 S. 2 BbgPolG; § 29 Abs. 6 S. 3 HSOG; § 34b Abs. 8 S. 5 SOG M-V (außer bei Personen, gegen die sich die Maßnahme richtete); § 30 Abs. 4 S. 4 Nds. SOG; § 17 Abs. 5 S. 2 PolG NRW; § 28 Abs. 5 S. 2 SPolG; § 186 Abs. 4 S. 2 LVwG (nur für unvermeidbar betroffene Dritte).

nahme gegenüber dieser Person, des Aufwands für die Feststellung ihrer Identität sowie der daraus für diese oder andere Personen folgenden Beeinträchtigung geboten ist."

Die Zurückstellung der Unterrichtung bedarf der richterlichen Zustimmung in Rheinland-Pfalz vor Ablauf von zwölf Monaten[266] und in elf Bundesländern innerhalb von sechs Monaten[267]. Stattdessen ist gemäß § 29 Abs. 6 S. 6 HSOG der Hessische Datenschutzbeauftragte spätestens sechs Monate nach Abschluss der Maßnahme in Kenntnis zu setzen. Keine vergleichbaren Beteiligungen sind in § 29 Abs. 7 BbgPolG, § 28 Abs. 5 SPolG und § 17 Abs. 7 SOG LSA enthalten. In fünf Bundesländern kann die Benachrichtigung mit richterlicher Zustimmung bei Vorliegen bestimmter, in den Ländern sehr unterschiedlich geregelter Voraussetzungen[268] auch dauerhaft unterbleiben. Eine Spezialregelung für die Benachrichtigung von Minderjährigen war nur in § 29 Abs. 7 S. 3

266 § 40 Abs. 5 S. 5 POG.

267 Art. 34 Abs. 6 S. 3 BayPAG; § 23 Abs. 6 S. 3 PolG BW; § 25 Abs. 7 S. 6 ASOG Bln; § 33 Abs. 5 S. 2 BremPolG; § 10a Abs. 6 S. 2 PolDVG HA; § 34b Abs. 8 S. 2 SOG M-V; § 30 Abs. 5 S. 3 Nds. SOG; § 17 Abs. 6 S. 1 PolG NRW; § 41 Abs. 8 S. 3 SächsPolG; § 186 Abs. 4 S. 5 LVwG; § 36 Abs. 5 S. 1 ThürPAG.

268 Art. 34 Abs. 6 S. 5 BayPAG: „wenn 1. überwiegende Interessen eines Betroffenen entgegenstehen oder 2. die Identität oder der Aufenthaltsort eines Betroffenen nur mit unverhältnismäßigem Aufwand ermittelt werden kann.";
§ 23 Abs. 6 S. 5 PolG BW: „wenn 1. überwiegende Interessen einer betroffenen Person entgegenstehen oder 2. die Identität oder der Aufenthalt einer betroffenen Person nur mit unverhältnismäßigem Aufwand ermittelt werden können oder 3. seit Beendigung der Maßnahme fünf Jahre verstrichen sind.";
§ 10a Abs. 6 S. 6 und 7 PolDVG HA: „wenn 1. die Voraussetzungen des Satzes 1 (d.h. ohne Gefährdung des Zwecks der Datenerhebung geschehen kann, Anm. des Evaluationsteams) auch nach fünf Jahren seit Beendigung der Maßnahme noch nicht eingetreten sind, 2. die Voraussetzungen des Satzes 1 (d.h. ohne Gefährdung des Zwecks der Datenerhebung geschehen kann, Anm. des Evaluationsteams) mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft nicht eintreten werden und 3. die Voraussetzungen für eine Löschung sowohl bei der Polizei als auch bei den Empfängern von Datenübermittlungen vorliegen. Mit Ausnahme der Personen, gegen die sich die Datenerhebungen richteten, kann eine Unterrichtung mit Zustimmung des nach S. 4 zuständigen Gerichts auch dann unterbleiben, wenn sie nur mit unverhältnismäßigen Ermittlungen möglich wäre oder wenn ihr überwiegende schutzwürdige Belange anderer Betroffener entgegenstehen.";
§ 41 Abs. 8 S. 5 SächsPolG: „wenn 1. überwiegende Interessen eines anderen Betroffenen entgegenstehen oder 2. deren Identität oder Aufenthaltsort nur mit unverhältnismäßigem Aufwand ermittelt werden kann.";
§ 186 Abs. 4 S. 9 LVwG: „Ist die Benachrichtigung für insgesamt fünf Jahre zurückgestellt worden und ergibt sich, dass die Voraussetzungen für eine Benachrichtigung

und 4 BbgPolG ersichtlich. Danach treten die Personensorgeberechtigten an die Stelle der Minderjährigen, jedoch kann von einer Benachrichtigung abgesehen werden, solange zu befürchten ist, dass sie zu erheblichen Nachteilen für den Minderjährigen führt.

3.3 Rechtliche Bewertung

3.3.1 Allgemeine Aspekte

3.3.1.1 Gefahrenabwehr und Strafverfolgung

Während die Verhütung von Straftaten der Gefahrenabwehr zuzurechnen ist, dient die Strafverfolgungsvorsorge der zukünftigen Durchführung der Strafverfolgung[269] und ist kompetenzmäßig dem „gerichtlichen Verfahren“ i.S.d. Art. 74 Abs. 1 Nr. 1 GG zuzuordnen[270], mithin dem Bereich der konkurrierenden Gesetzgebung[271]. Ob der Bundesgesetzgeber eine abschließende Regelung getroffen hat, bestimmt sich nach dem konkreten Einzelfall.[272] Insoweit bleibt es unschädlich, wenn die Länder Maßnahmen zur Verhinderung künftiger Straftaten vorsehen, die auch deren Verfolgung dienen können.[273]

Viele Entscheidungen des BVerfG ergingen im Zusammenhang mit Maßnahmen der Strafverfolgung. Dadurch ist problematisch, inwiefern die in diesen Entscheidungen entwickelten Grundsätze auch für die entsprechenden

---

mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft nicht eintreten werden, kann mit Zustimmung des mit der Sache bereits befassten Landgerichts von einer Benachrichtigung endgültig abgesehen werden.“;
§ 36 Abs. 5 S. 3 ThürPAG: „Aufgrund richterlicher Entscheidung kann von einer Benachrichtigung endgültig abgesehen werden, wenn die Voraussetzungen dafür mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft nicht eintreten werden.“.

269 Vgl. BVerwG, NVwZ 2012, 757, 760, Rn. 32.

270 Vgl. BVerfG, NJW 2005 2603, 2605; BVerwG NVwZ 2012, 757, 760, Rn. 33.

271 Vgl. BVerfG, NJW 2005 2603, 2605.

272 Bejaht von BVerfG NJW 2005, 2603, 2606 für den Bereich der Telekommunikation.

273 Vgl. BVerwG NVwZ 2012, 757, 760; Würtenberger, in: Ehlers/ Fehling/ Pünder, Verwaltungsrecht 3, § 69 Rn. 310. Vgl. auch VerfG LSA, Urt. v. 11.11.2014 – LVG 9/13, Entscheidungsgründe, Ziff. 2.2.2.

Bestimmungen der Gefahrenabwehr fruchtbar gemacht werden können. Teilweise wird dem präventiven polizeilichen Schutz im Rahmen einer Abwägung mit Rechtsgütern des individuell Betroffenen eine höhere Bedeutung zugemessen als den Maßnahmen der Strafverfolgung.[274] Bei Zugrundelegung einer solchen Betrachtung wären die vom BVerfG an Strafverfolgungsvorschriften angelegten, aus den Grundrechten abgeleiteten Grenzen für den Bereich der Gefahrenabwehr leichter überwindbar. Gegen die Zulässigkeit einer solchen pauschalierenden Betrachtungsweise spricht aber, dass das BVerfG der Strafrechtspflege einen hohen Stellenwert zugeschrieben hat. So führt es aus:

> *„Das Rechtsstaatsprinzip gestattet und verlangt die Berücksichtigung der Belange einer funktionstüchtigen Strafrechtspflege, ohne die der Gerechtigkeit nicht zum Durchbruch verholfen werden kann.“*[275]

Richtigerweise wird in jedem Einzelfall zu überprüfen sein, ob bzw. inwieweit die Grundsätze, die das BVerfG für Strafverfolgungsmaßnahmen aufgestellt hat, auf den Bereich der Gefahrenabwehr übertragbar sind. Ein Gleichlauf ergibt sich jedenfalls dort, wo eine Abwägung aus Gründen der Menschenwürde nicht möglich ist. Die Entscheidungen zum Kernbereich privater Lebensgestaltung gelten daher für Gefahrenabwehr und Strafverfolgung gleichermaßen.[276]

---

274 Vgl. *Ebert/ Seel*, ThürPAG, § 35 Rn. 2; *Schmidbauer*, in: Schmidbauer/ Steiner, BayPAG, Art. 34a Rn. 79; *Bode*, NJ 2005, S. 5, 9; a.A. *Möstl*, DVBl. 2010, 808, 812. Siehe auch BVerfG, NJW 2000, 55, 66: „Da im Fall der Strafverfolgung die Verletzung des Rechtsguts bereits stattgefunden hat und es nunmehr um die Sanktion geht, ist es nicht gerechtfertigt, die Übermittlungsschwelle für personenbezogene Daten, die aus Eingriffen in das Fernmeldegeheimnis gemäß §§ 1, 3 G 10 stammen, unter diejenige abzusenken, welche auch sonst bei der Strafverfolgung für Eingriffe in das Fernmeldegeheimnis nach § StPO gilt.“

275 Vgl. BVerfG NStZ 2011, 103, 104.

276 Vgl. BVerfG NJW 2008, 822, 832; BVerfG NJW 2004, 999, 1002; *Ebert/ Seel*, ThürPAG, § 35 Rn. 2; *Petri*, in Lisken/ Denninger, Handbuch, Kapitel G, Rn. 29; a.A. noch *Haas* NJW 2004, 3082, 3084.

3.3.1.2 Verwaltungsgerichtliche Zuständigkeit bei Richtervorbehalten

3.3.1.2.1 Allgemeines

Von den zu evaluierenden Maßnahmen ist beim Richtervorbehalt nur für die Rasterfahndung gemäß § 38 Abs. 3 S. 2 POG das Amtsgericht zuständig. Diese Zuweisung entspricht den anderen Bundesländern, soweit diese für jene Maßnahme überhaupt einen Richtervorbehalt statuiert haben (→Kapitel 3.2.9.2, S. 48). Rechtliche Bedenken gegen diese Regelung sind nicht ersichtlich.

Erörterungsbedürftig ist allerdings die (landesrechtliche) Zuweisung der richterlichen Kontrolle an die Verwaltungsgerichtsbarkeit[277], mitsamt der Regelung, dass das OVG nach Maßgabe der VwGO entscheide, und speziell die Verweisung an das OVG Rheinland-Pfalz in erstinstanzlicher Zuständigkeit. Dies gilt für die Maßnahmen der Wohnraum-, der Telekommunikationsüberwachung, der Quellen-TKÜ, der Auskunft über Nutzungsdaten, der Online-Durchsuchung und der Funkzellenabfrage.[278] Demgegenüber wird in den meisten anderen Bundesländern das Amtsgericht und vereinzelt das Landgericht für zuständig erklärt[279]. Noch unproblematisch ist dabei der Umstand, dass das OVG erstinstanzlich zuständig ist und auch letztinstanzlich entscheidet.[280]

3.3.1.2.2 Anwendbarkeit der VwGO durch Verweisung?

Die Zuweisung der Aufgaben an den Verwaltungsrechtsweg und die Erklärung, dass die VwGO anwendbar ist, werden teilweise als nichtig angesehen. Nach herrschender Auffassung sind konstitutiv aufdrängende Sonderzuweisungen durch Landesrecht nicht regelbar.[281] § 40 Abs. 1 S. 2 VwGO enthält eine Öff-

---

277 *Ruthig*, in: Landesrecht Rh-Pf, § 4 Rn. 138 betrachtet die Verlagerung der Zuständigkeit auf die Verwaltungsgerichtsbarkeit als zulässig.

278 Vgl. § 29 Abs. 7 S. 1, 2; § 31 Abs. 5 S. 1, 2; § 31b Abs. 2 S. 2 iVm § 31 Abs. 5 S. 1, 2; § 31c Abs. 5 S. 2, 3; § 31e Abs. 2 S. 2 Halbs. 1 iVm § 31 Abs. 5 S. 1 und 2 POG.

279 Für die Wohnraumüberwachung: siehe Kapitel 3.2.2.2, S. 23.
Für die Telekommunikationsüberwachung: siehe Kapitel 3.2.3.3, S. 32.

280 Vgl. *Scheidler*, in: Gärditz, VwGO, § 48 Rn. 5; vgl. auch die Gesetzesbegründung, Landesregierung, LT-Drs. 15/4879, S. 30.

281 Vgl. *v. Albedyll*, in: Bader u.a., VwGO, § 40 Rn. 122; *Haack*, in: Gärditz, VwGO, § 40 Rn. 7; *Unruh*, in: Hk-VerwR, § 40 VwGO Rn. 35 f; vgl. auch *Oeter*, in: v. Mangoldt/

nungsklausel für abdrängende Sonderzuweisungen. Aufdrängende Sonderzuweisungen finden sich in anderen, bundesgesetzlich geregelten Vorschriften.[282] Der Bund hat insoweit von seiner konkurrierenden Gesetzgebungskompetenz (vgl. Art. 72 Abs. 1, Art. 74 Abs. 1 Nr. 1 GG) abschließend Gebrauch gemacht.[283] Die Sperrwirkung des Art. 72 Abs. 1 GG bewirkt die Nichtigkeit der Vorschrift.[284] Es ist nicht erforderlich, dass die Norm inhaltlich dem Bundesrecht widerspricht.[285] Nach anderer Auffassung hat die Vorschrift deklaratorischen Charakter,[286] während nach dritter Auffassung eine wirksame konstitutive Verweisung vorliegt, sofern der Verwaltungsrechtsweg eröffnet ist.[287] In allen drei Fällen – auch bei unterstellter Nichtigkeit der Zuweisung – gilt aber, dass die VwGO anwendbar ist, wenn die Voraussetzungen des § 40 Abs. 1 S. 1 VwGO vorliegen.

Eine Auffassung hält die Eröffnung des Verwaltungsrechtswegs nicht für gegeben, da keine „Streitigkeit“ vorliege.[288] Der Bürger werde vor der richterlichen Anordnung nicht angehört, sondern erst nachträglich. Dementsprechend könne er auch noch keine Rechtsbehelfe gegen die Maßnahme einlegen. Diese Ansicht verkennt, dass es auf das Vorliegen eines Rechtsstreits nicht ankommt. Auch § 13 GVG spricht von einer Streitigkeit. Im Ergebnis wäre für Richtervorbehalte also weder der Rechtsweg zu den Verwaltungs- noch zu den ordentlichen Gerichten gegeben – ein sinnwidriges Ergebnis.

Für Richtervorbehalte ist der Verwaltungsrechtsweg gegeben. Dafür spricht, dass durch die richterliche Anordnung ausschließlich ein Träger öffentlicher Gewalt (nämlich die Polizeibehörde) zu Maßnahmen berechtigt wird.[289] Mithin liegt eine öffentlich-rechtliche Streitigkeit vor. Für den Verwaltungsrechtsweg spricht auch der Gleichklang mit den Möglichkeiten des nachträglichen

---

Klein/ Starck, GG, Band 2, Art. 74 Rn. 27; unklar bei *Ruthig*, in: Landesrecht Rh-Pf, § 4 Rn. 138.

282 Vgl. *Sodan*, in: Sodan/ Ziekow, VwGO, § 40 Rn 134 ff.

283 Vgl. BVerfG NJW 1991, 1283.

284 Vgl. *Unruh*, in: Hk-VerwR, § 40 VwGO, Rn. 37.

285 Vgl. *Jarass*, in: Jarass/ Pieroth, GG, Art. 72 Rn. 11a; *Oeter*, in: v. Mangoldt/ Klein/ Starck, Band 2, Art. 72, Rn. 27; *Uhle*, in: Maunz/ Dürig, GG, Art. 72 Rn. 118; BVerfG NVwZ 2000, 1160.

286 Vgl. *v. Albedyll*, in: Bader, VwGO, § 40 Rn. 122.

287 Vgl. *Sodan*, in: Sodan/ Ziekow, VwGO, § 40 Rn. 140.

288 Vgl. *Aschmann*, Richtervorbehalt, S. 63.

289 Vgl. zu den Theorien *Sodan/ Ziekow*, Grundkurs, § 67 Rn. 6-9.

Rechtsschutzes. Denn insoweit ist das Verwaltungsgericht zuständig, selbst wenn der Richtervorbehalt den Amtsgerichten zugewiesen ist.[290] Ähnlich argumentiert das VG Stade für eine richterliche Durchsuchungsanordnung zur Durchsetzung der Musterung von Wehrpflichtigen nach § 44 Abs. 2 WPflG.[291]

3.3.1.2.3 Zuweisung zum OVG Rheinland-Pfalz durch Landesrecht?

Die Zuweisung zum OVG ist insoweit problematisch, als gemäß § 45 VwGO in erster Instanz grundsätzlich das Verwaltungsgericht zuständig ist. Die VwGO basiert auf der konkurrierenden Gesetzgebungskompetenz des Bundes gemäß Art. 74 Abs. 1 Nr. 1 GG für die Gerichtsverfassung und das gerichtliche Verfahren. Danach besteht die Gesetzgebungszuständigkeit nur unter den Voraussetzungen des Art. 72 GG, ansonsten ist die Gesetzgebungskompetenz der Länder begründet. Mit Erlass der VwGO hat der Bund von der Kompetenz Gebrauch gemacht, Verfassung und Verfahren der Verwaltungsgerichte zu regeln und dabei das Verfahren der Verwaltungsgerichte erschöpfend geregelt.[292] Nach allgemeiner Ansicht in der Literatur[293] ist eine abweichende instanzielle Zuweisung durch Landesgesetz ausgeschlossen, soweit nicht der Bundesgesetzgeber eine Öffnungsklausel zugunsten der Landesgesetzgeber erlassen hat.[294] Dies wird durch die Gesetzesbegründung zur VwGO gestützt, wonach damals noch bestehende Zuständigkeiten des OVG in Bayern, Bremen, Rheinland-Pfalz und Württemberg-Baden abgeschafft wurden und Ausnahmen nur noch in bestimmten, genau in der VwGO aufgezählten Fällen bestehen sollten.[295] Auch im weiteren Verfahren stimmte der Rechtsausschuss

---

290 Vgl. den Überblick bei *Ehlers/ Schneider*, in: Schoch/ Schneider/ Bier, VwGO, § 40 Rn. 614 ff.

291 Vgl. VG Stade, NVwZ 2004, 124. Dagegen spricht auch nicht der § 35 WPflG. Denn dieser besagt: „Für *Rechtsstreitigkeiten* bei der Ausführung dieses Gesetzes ist der Verwaltungsrechtsweg gegeben." Das Problem, ob eine Streitigkeit vorliegt, wird dadurch also nicht gelöst. In der Entscheidung des VG Berlin NVwZ 2012, 167 f. wurde die richterliche Anordnung im Wege der Verwaltungsvollstreckung zur Durchsetzung einer Forderung begehrt, eine Streitigkeit lag also bereits vor, vgl. auch VG Ansbach, Beschluss vom 28.03.2013 – AN 15 X 13.00641.

292 BVerfG NJW 1974, 1812, 1813; BVerwGE 54, 29, 34.

293 In diesem Sinne: *v. Albedyll*, in: Bader u.a., VwGO, § 45 Rn. 3; *Bier/ Schenk*, in: Schoch/ Schneider/ Bier, § 45 Rn. 2 in Fn. 5; *Kugele*, VwGO, § 45 Rn. 3; *Ziekow*, in: Sodan/Ziekow, VwGO, § 45 Rn. 8; a. M. *Lücke*, JuS 1961, 41, 42 in der Fußnote 17.

294 Solche Öffnungsklauseln finden sich in § 47 Abs. 1 Nr. 2 und § 48 Abs. 1 S. 3 VwGO.

295 BT-Drs. 3/55 S. 33.

für eine abschließende Regelung, „damit landesrechtlich keine abweichenden Vorschriften über die sachliche Zuständigkeit des Verwaltungsgerichts erlassen werden können. Die Verwaltungsgerichte entscheiden hiernach im 1. Rechtszug auch über Verwaltungsakte der Ministerien im Gegensatz zu der bisherigen Regelung in den meisten süddeutschen Verwaltungsgerichtsgesetzen.“[296]

Ein Vorbehalt für den Landesgesetzgeber zur Regelung der instanziellen Zuständigkeit ist angesichts der zitierten Gesetzesbegründungen zur VwGO unwahrscheinlich. Dementsprechend war es dem Landesgesetzgeber in Rheinland-Pfalz nicht möglich, in der Gesetzesbegründung auf eine Öffnungsklausel des Bundesgesetzgebers hinzuweisen, die eine Zuständigkeit des Oberverwaltungsgerichts ermöglicht hätte.[297] In der parlamentarischen Debatte konnten nur Hinweise auf die Zweckmäßigkeit der Zuweisung zum Oberverwaltungsgericht gefunden werden.[298] Sonstige Recherchen blieben ergebnislos.

In der Gesetzesbegründung heißt es bezüglich der zu evaluierenden Vorschriften lediglich:

> *„Für diese Fälle soll durch die Verlagerung der bisherigen Zuständigkeit der Amtsgerichte auf das Oberverwaltungsgericht Rheinland-Pfalz die Wirksamkeit des Richtervorbehalts akzentuiert werden, da für die richterliche Beurteilung derart intensiver Grundrechtseingriffe profunde Kenntnisse des Verfassungs- und Verwaltungsrechts sowie entsprechende Erfahrungen förderlich sind.“ Dabei „ist es folgerichtig, wenn das Gericht, wie auch in sonstigen polizeirechtlichen Streitigkeiten, nach Maßgabe der Verwaltungsgerichtsordnung entscheidet.“*[299]

3.3.1.2.4 Richtervorbehalt als unzulässige Verwaltungsgeschäfte?

Ein generelles Problem ist, ob es sich bei den richterlichen Anordnungen um Verwaltungsgeschäfte handelt. Höchstrichterliche Rechtsprechung zu dieser Streitfrage ist noch nicht vorhanden. Teilweise wird die Ansicht vertreten, § 39

296 BT-Drs. 3/1094, S. 5.

297 Vgl. Landesregierung, LT-Drs. 15/4879, S. 30.

298 Vgl. Plenarprotokoll 15/105, S. 6233 f.

299 Landesregierung, LT-Drs. 15/4879, S. 30.

VwGO stehe der Zuweisung des Richtervorbehalts an die Verwaltungsgerichte entgegen.[300] Danach heißt es: „Dem Gericht dürfen keine Verwaltungsgeschäfte außerhalb der Gerichtsverwaltung übertragen werden.“ Durch die richterliche Anordnung erfolge ein Eingriff in die Rechte des Bürgers. Verwaltungsgerichte seien jedoch für den Rechtsschutz für den Bürger zuständig.[301] Dieses Problem wurde auch im Innenausschuss angesprochen.[302] Gefolgt wurde der herrschenden Lehre, wonach der Übertragung von Richtervorbehalten auf die Verwaltungsgerichtsbarkeit die Regelung in § 39 VwGO nicht entgegensteht.[303] Der Richter entscheide aufgrund von § 1 VwGO in sachlicher und persönlicher Unabhängigkeit und daher nicht als Teil der Verwaltung.[304] Während sich § 39 VwGO an die Verwaltungsgerichte richtet, betrifft § 4 DRiG die Aufgaben des einzelnen Richters. In § 4 Abs. 2 Nr. 2 DRiG wird teilweise eine Sondervorschrift gesehen.[305] In der Bestimmung heißt es:

> *„Außer Aufgaben der rechtsprechenden Gewalt darf ein Richter jedoch wahrnehmen…* 2. *andere Aufgaben, die auf Grund eines Gesetzes Gerichten oder Richtern zugewiesen sind…“*

Die Zuweisung von Aufgaben kann durch Bundes- oder Landesgesetz erfolgen.[306] Für die Einordnung der Tätigkeit unter § 4 Abs. 2 DRiG ist entscheidend, dass es sich bei straf- und polizeirechtlichen Richtervorbehalten nicht um traditionelle Rechtsprechungstätigkeit handelt.[307] In Betracht kommt daher nur die Zuweisung einer rechtsprechenden Aufgabe durch den Gesetzgeber. Dabei ist das Gewaltenteilungsprinzip zu beachten. Die drei Voraussetzungen,

---

300 Vgl. VG Osnabrück, NdsVBl 1994, 64.

301 Vgl. VG Osnabrück, NdsVBl 1994, 64, 65.

302 Vgl. *Ruthig*, 41. Sitzung des Innenausschusses am 04.11.2010, Teil II, S. 31.

303 Vgl. *Berlit*, NdsVBl 1995, 197, 201; *Wittreck*, in: Gärditz, VwGO, § 39 Rn. 3; *Ruthig*, Kernbereich, S. 516; *Aschmann*, Richtervorbehalt, S. 62; *Lüdemann* DÖV 1996, 870, 874; a.A. *Kugele*, VwGO, § 39 Rn. 4 und *Kopp/ Schenke*, VwGO, § 39 Rn. 3, wonach im Einzelfall zu beurteilen ist, ob der Richtervorbehalt Verwaltungstätigkeit darstellt.

304 Vgl. *Berlit*, NdsVBl 1995, 197, 201.

305 Vgl. *Kimmel*, in: Posser/ Wolf, VwGO, § 39 Rn.4; *Lüdemann* DÖV 1996, 870, 873, wonach der § 39 VwGO so auszulegen ist, dass er § 4 Abs. 2 DRiG nicht widerspricht; *Guckelberger*, in: Sodan/ Ziekow, VwGO, § 39 Rn. 6, wonach lediglich zu beachten ist, dass nicht in den Kernbereich von Rechtsprechung oder Verwaltung eingegriffen wird.

306 Vgl. *Schmidt-Räntsch*, DRiG, § 4 Rn. 32; BVerwG NJW 1985, 1093, 1094.

307 Vgl. von *Kühlewein*, Richtervorbehalt, S. 267.

die das BVerfG aufgestellt hat (→ Kapitel 3.3.10.4.2, S. 137) sind erfüllt.[308] Darüber hinaus fordert das BVerwG, dass dem Richter nur Aufgaben zugewiesen werden dürfen, die eine sachliche Nähe zu seiner richterlichen Tätigkeit haben und für deren Wahrnehmung er beruflich erworbene, für die Tätigkeit erwünschte Voraussetzungen in Form von Erfahrungen und Sachverstand mit sich bringt.[309] Da der nachträgliche Rechtsschutz gegen polizeiliche Maßnahmen ebenfalls bei den Verwaltungsgerichten, in der Berufungsinstanz beim OVG angesiedelt ist, kann die sachliche Nähe des Richtervorbehalts für die zu evaluierenden Normen bejaht werden.

3.3.1.2.5 Organisatorische Sicherstellung der Regelzuständigkeit des Gerichts

Der Gedanke, dass im Rahmen der Strafverfolgung die staatlichen Organe verpflichtet sind, die effektive Durchsetzung des grundrechtssicherenden Richtervorbehalts zu gewährleisten[310] und die entsprechend vorgesehene Regelzuständigkeit zu wahren[311], lässt sich auch aufs Gefahrenabwehrrecht übertragen. Richtervorbehalte müssen auch in ihrer konkreten Ausgestaltung die organisatorischen Anforderungen an eine zeit- und sachangemessene Wahrnehmung der dem Richter übertragenen Kontrollbefugnisse gewährleisten[312], was die Möglichkeit einer unverzüglichen richterlichen Entscheidung miteinschließt, auch nachts und am Wochenende.[313]

3.3.1.3 Verwendung der Daten für andere Zwecke § 29 Abs. 5 POG (i.V.m. § 31 Abs. 7 S. 1, § 31b Abs. 4, § 31c Abs. 6, § 31e Abs. 2 S. 2 Halbs. 2 POG)

Die Verwendung personenbezogener Daten für andere Zwecke ist nur unter jeweils besonders vorgeschriebenen Voraussetzungen zulässig.

---

308 Vgl. *Aschmann*, Richtervorbehalt, S. 164; a.A. *Rachor*, in: Lisken/ Denninger, Handbuch, Kap. C, Rn. 35.

309 Vgl. BVerwG NJW 1985, 1093, 1094; Staats, DRiG, § 4 Rn. 14.

310 Vgl. BVerfG, Urt. v. 16.06.2015 – 2 BvR 2718/10 u.a., Rn. 62.

311 Vgl. BVerfG, Urt. v. 20.02.2001 – 2 BvR 1444/00, Rn. 37.

312 *Ruthig*, in: Landesrecht Rh-Pf, § 4 Rn. 138.

313 *Ruthig*, in: Landesrecht Rh-Pf, § 4 Rn. 138, Fn. 213.

Als Problem der Normenbestimmtheit und Normenklarheit stellt sich der Verweis auf § 29 Abs. 5 POG für die TKÜ, die Quellen-TKÜ, die Auskunft über Nutzungsdaten, die Online-Durchsuchung und die Funkzellenabfrage dar. Diese Vorschrift betrifft die Regelung über eine Zweckänderung der Daten. Der 69. Deutsche Juristentag 2012 gab inzwischen die Beschlussempfehlung, die Online-Durchsuchung wieder in der StPO zu normieren.[314] In den §§ 31 Abs. 7 S. 1, § 31b Abs. 4, § 31c Abs. 6 und § 31e Abs. 2 S. 2 Halbs. 2 POG heißt es:

> *„§ 29 Abs. 5 (und 8) findet entsprechende Anwendung."*

Dabei geht aus dem Wortlaut nicht hervor, wie weit diese Entsprechung gilt. § 29 Abs. 5 S. 2 POG regelt:

> *„Solche Daten dürfen für einen anderen Zweck verwendet werden, soweit dies zur 1. Verfolgung von besonders schweren Straftaten, die nach der Strafprozessordnung die Wohnraumüberwachung rechtfertigen, 2. Abwehr einer dringenden Gefahr im Sinne des Absatzes 1 erforderlich ist. Die Zweckänderung muss im Einzelfall festgestellt und dokumentiert werden."*

Nach dem Wortlaut der Vorschrift könnte eine Zweckänderung nur dann zulässig sein, wenn es der Verfolgung von besonders schweren Straftaten i.S.d. § 100c Abs. 2 StPO dient. Die Gesetzesbegründung zu § 31d POG verweist auf die fehlende Normierung einer Online-Durchsuchung in der StPO, wodurch § 161 Abs. 2 StPO eine Zweckänderung für die Strafverfolgung zurzeit verhindere.[315] Dies deutet darauf hin, dass der Gesetzgeber mit dem Verweis ausdrücken möchte, dass sich die Zweckänderung *allein* nach § 161 Abs. 2 StPO richtet. Danach ist eine Verwendung der Daten zur Strafverfolgung gemäß § 161 Abs. 2 StPO dann zulässig, wenn der Betroffene einwilligt oder die Voraussetzungen ihrer Anordnung zum Zwecke der Strafverfolgung in der StPO von vornherein gegeben wären. Dies entspräche auch der Auffassung des BVerfG.[316] Problematisch hierbei ist jedoch, dass dies weder aus dem Wortlaut der Vorschrift noch aus der Gesetzesbegründung eindeutig hervorgeht. Die Strafverfolgungsbehörden müssen für eine Zweckänderung polizeirechtlich

---

314 Vgl. Beschlüsse, 69. Deutscher Juristentag 2012, S. 14.

315 Vgl. Landesregierung, LT-Drs. 15/4879, S. 39.

316 Vgl. BVerfG NJW 2012, 907, 913 m.w.N.; BVerfG NJW 2013, 1499, 1517; BVerfG NJW 2004, 2213, 2220.

erlangter Daten die Anforderungen des § 161 Abs. 2 StPO beachten. Die „entsprechende Anwendung“ des § 29 Abs. 5 POG könnte auch dahingehend verstanden werden, dass zusätzlich zu den Voraussetzungen des § 161 Abs. 2 StPO eine besonders schwere Straftat gemäß § 100c Abs. 2 StPO vorliegen muss. Diesem zusätzlichen Erfordernis steht die bundesstaatliche Kompetenzordnung nicht entgegen. Nach Art. 72 Abs. 1, 74 Abs. 1 Nr. 1 GG ist entscheidend, ob der Bundesgesetzgeber von seiner Kompetenz abschließend Gebrauch gemacht hat. In dem Gesetzesentwurf der Bundesregierung zur Neufassung des § 161 StPO heißt es aber nur:

> *„Werden Daten aus vergleichbaren Maßnahmen nach anderen Gesetzen (etwa den Polizeigesetzen oder den Gesetzen über die Nachrichtendienste) in das Strafverfahren eingeführt, so gilt das auch für deren Verwendung, um einer Umgehung der engen strafprozessualen Anordnungsvoraussetzungen vorzubeugen.“*[317]

Diese Formulierung deutet darauf hin, dass der Gesetzgeber hier Mindestanforderungen geregelt hat, über die das Polizeirecht auch hinausgehen kann.

Verdeutlicht sei das Problem an Daten, die aus einer Telekommunikationsüberwachung gewonnen wurden und für Zwecke der Strafverfolgung verwendet werden sollen. Eine dem Wortlaut des § 29 Abs. 5 S. 2 Nr. 1 POG entsprechende Anwendung über § 31 Abs. 7 S. 1 POG würde zu dem (sinnwidrigen) Ergebnis führen, dass für die Verwendung der Daten zur Strafverfolgung eine Katalogtat nach § 100c Abs. 2 StPO vorliegen und wegen § 161 Abs. 2 StPO *zusätzlich* die Voraussetzungen einer Anordnung nach § 100a StPO gegeben sein müssten. Der Sinn einer solchen doppelten Inbezugnahme wäre kaum erkennbar, da sich die Kataloge in § 100a Abs. 2 StPO und § 100c Abs. 2 StPO teilweise decken. Stellt man daher auf Sinn und Zweck der Regelung ab, so führt die „*entsprechende* Anwendung“ des § 29 Abs. 5 POG dazu, dass nicht zusätzlich die Anforderungen der StPO an die Rechtfertigung einer Wohnraumüberwachung, sondern immer nur die Anforderungen der StPO an die Rechtfertigung der *jeweiligen*, nach dem POG ergriffenen Maßnahme vorliegen müssen[318]. Dies heißt konkret u.a., dass für jede neue Nutzung der Daten

---

317 Vgl. Bundesregierung, BT-Drs. 16/5846, S. 64, wobei dies auf dem Gedanken des hypothetischen Ersatzeingriffs beruht.

318 Vgl. insoweit auch BVerfG, Urt. v. 20.04.2016, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09, Rn. 288: „Voraussetzung für eine Zweckänderung ist […], dass die neue Nutzung der Daten dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts dient, die verfassungsrechtlich ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnten“, und Rn. 290:

aus einer Wohnraumüberwachung oder einem Zugriff auf informationstechnische Systeme angesichts des besonderen Eigengewichts dieser Maßnahmen entsprechend den Anforderungen, welche an eine Datenneuerhebung gestellt würden, eine dringende Gefahr bzw. eine hinreichend konkretisierte Gefahr vorliegen muss.[319] Aus einer teleologischen Auslegung ergibt sich also, dass die entsprechende Anwendung nicht zusätzlich den Straftatenkatalog nach § 100c Abs. 2 StPO erfasst.

Wie die geführten Interviews gezeigt haben (→ Kapitel 4.2.5, S. 195), ist dieser Zusammenhang aus den Normen allerdings nicht ohne weiteres zu erschließen. Die Anforderungen an die Bestimmtheit gesetzlicher Regelungen richten sich nach der Intensität der grundrechtlich betroffenen Bereiche.[320] Durch die Weiterverwendung der Daten wird in das Recht auf informationelle Selbstbestimmung eingegriffen. Es bestehen daher Bedenken, ob die Normenbestimmtheit der Vorschriften gewährleistet ist, soweit sie § 29 Abs. 5 POG für entsprechend anwendbar erklären.

3.3.1.4 Additive Grundrechtseingriffe und Rundumüberwachung

Mehrere für sich betrachtet möglicherweise angemessene oder zumutbare Eingriffe in grundrechtlich geschützte Bereiche können in ihrer Gesamtwirkung zu einer schwerwiegenden Beeinträchtigung führen, die das Maß der rechtsstaatlich hinnehmbaren Eingriffsintensität überschreitet.[321] Eine Unzulässigkeit kann sich daraus ergeben, dass verschiedene Maßnahmen gleichzeitig gegen denselben Adressaten durchgeführt werden, einen vergleichbaren Gegenstand betreffen und in Grundrechte des Adressaten eingreifen.[322] Dieses Problem wird mit den Stichworten der Rundumüberwachung bzw. den additiven/kumulativen Grundrechtseingriffen umschrieben.

„Der Gesetzgeber kann [...] eine Zweckänderung grundsätzlich dann erlauben, wenn es sich um Informationen handelt, aus denen sich im Einzelfall konkrete Ermittlungsansätze zur Aufdeckung von vergleichbar gewichtigen Straftaten oder zur Abwehr von zumindest auf mittlere Sicht drohenden Gefahren für vergleichbar gewichtige Rechtsgüter wie die ergeben, zu deren Schutz die entsprechenden Datenerhebungen zulässig sind."

319 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09, Rn. 291.

320 Vgl. *Sommermann*, in: Mangoldt/Klein/Starck, GG, Band 2, Art. 20 Rn. 291.

321 Vgl. BVerfG NJW 2012, 1784, 1785 f.

322 Vgl. *Kirchhof*, NJW 2006, 732, 734.

Der gleichzeitige Einsatz mehrerer technischer Mittel ist nicht schlechthin unzulässig.[323] Es kann jedoch ein Verstoß gegen die Menschenwürde darstellen, wenn eine jedenfalls längerfristige zeitliche und räumliche „Rundumüberwachung" stattfindet. Denn die Wahrscheinlichkeit ist *groß, dass dabei höchstpersönliche Gespräche abgehört werden.*[324] *Die Überwachung verletzt die Menschenwürde jedenfalls dann, wenn sie so umfassend ist, dass nahezu lückenlos alle Bewegungen und Lebensäußerungen des Betroffenen registriert werden und zur Grundlage für ein Persönlichkeitsprofil werden können*[325]. Das kann auch dann der Fall sein, wenn etwa eine Online-Durchsuchung und eine TKÜ zusammen durchgeführt werden, um eine Vollüberwachung des Zielsystems zu erreichen.[326]

Der Gesetzgeber muss das Verbot einer Rundumüberwachung nicht ausdrücklich regeln[327], da es als Ausprägung des Verhältnismäßigkeitsgrundsatzes zur Wahrung eines in der Menschenwürde wurzelnden unverfügbaren Kerns der Person unmittelbar von Verfassungs wegen gilt und von den Sicherheitsbehörden im Rahmen ihrer Befugnisse von sich aus zu beachten ist[328]. Daher genügen die Vorschriften des POG insoweit den verfassungsrechtlichen Anforderungen.

3.3.1.5 Aufsichtliche Kontrolle

Das BVerfG hat verschiedene von ihm gesehene Unzulänglichkeiten der (die richterliche Aufsicht[329] ergänzenden) aufsichtlichen Kontrolle in seinem Urteil

---

323 Vgl. *Hegmann*, in: Graf, StPO, § 100c Rn. 4.

324 Vgl. BVerfG NJW 2004, 999, 1004.

325 Vgl. BVerfG, NJW 2004, 999, 1004; BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 u. 1140/09, Rn. 130.

326 Vgl. *Polenz*, in: Kilian/ Heussen, Handbuch, Teil 13, Rn. 39.

327 Vgl. BVerfG NJW 2007, 2753, 2757; zu den verfahrensrechtlichen Anforderungen vgl. BVerfG, Urt. v. 12.4.2005 – 2 BvR 581/01 zu § 100c StPO; vgl. auch BGH NJW 2009, 3448, 3458 f.

328 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09, Rn. 254.

329 Kritisch zu dem Umstand, dass das BVerfG (BVerfG, Urt. v. 20.04.2016 –1 BvR 966/09, BvG 1140/09, Rn. 117, 172-174, 207, 216, 235) „eigentlich unübersehbare Differenzierungen“ der Verfassung durch die Ausweitung ungeschriebener und aus dem Verhältnismäßigkeitsprinzip hergeleteiter Richtervorbehalte einebne, und die „Effektivität“ der Richtervorbehalte durch die „enorme Ausweitung“ geschwächt werde: *Durner*, DVBl. 2016, 780, 782 und 784.

zum BKAG auf der Grundlage des Verhältnismäßigkeitsgrundsatzes und dessen Anforderungen an Transparenz, individuellen Rechtsschutz und aufsichtliche Kontrolle[330] bemängelt.

So habe der Gesetzgeber für den Fall, dass die Erfassung kernbereichsrelevanter Informationen (→ Kapitel 3.3.10, S. 121 ff.) nicht vermieden werden könne, anschließend auf der Ebene der Auswertung in der Regel die Sichtung der erfassten Daten durch eine unabhängige Stelle vorzusehen[331]. In seinem Urteil zum BKAG hat das BVerfG dies für einige der von ihm geprüften Regelungsbereiche gefordert, nämlich, für die Wohnraumüberwachung[332] und für die Online-Durchsuchung[333], jedoch nicht für die Telekommunikationsüberwachung[334] oder die Erhebung von Telekommunikationsverkehrsdaten[335].

Für die Kontrolle nach den Vorschriften des Bundesdatenschutzgesetzes vermisst das BVerfG eine gesetzliche Vorgabe zu turnusmäßigen Pflichtkontrollen einer mit wirksamen Befugnissen ausgestatteten Stelle (wofür das BVerfG im Bereich des BKAG den Bundesdatenschutzbeauftragten nennt[336]), deren Abstand ein gewisses Höchstmaß, etwa zwei Jahre, nicht überschreiten dürfe[337] und wie sie auf eine entsprechende Rüge des BVerfG hinsichtlich des Fehlens einer entsprechenden Regel im ATDG[338] nunmehr in § 10 Abs. 2 ATDG eingefügt wurde[339].

---

330 BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09., Rn. 134.

331 BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09, Rn. 129, 204, 223-225. „Durch Rechtsstaatlichkeit und Transparenz“ des Modells überzeugt ist *Buchholtz*, NVwZ 2016, 906, 909. Die Maßnahme wird als „lebensfremd“ und als die Behördenarbeit erheblich verzögernd von *Wiemers*, NVwZ 2016, 839, 841, kritisiert; Zweifel an der Berechtigung des Verfassungsgerichts zu derartigen Ableitungen aus der Verfassung äußert *Durner*, DVBl. 2016, 780, 783.

332 BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/069 und 1 BvR 1140/09, Rn. 204.

333 BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/069 und 1 BvR 1140/09, Rn. 223-225.

334 BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/069 und 1 BvR 1140/09, Rn. 240-245.

335 BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/069 und 1 BvR 1140/09, Rn. 250, 240-245.

336 BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/069 und 1 BvR 1140/09, Rn. 141.

337 BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/069 und 1 BvR 1140/09, Rn. 141.

338 BVerfG, NJW 2013, 1499, 1517, Rn. 217.

339 Mit Artikel 1 Nr. 9 b des Gesetzes zur Änderung des Antiterrordateigesetzes und anderer Gesetze vom 18.12.2014 (BGBl 2014 I 2318); vgl. Begründung des Änderungsgesetzesentwurfs BT-Drs. 18/1565 S. 20.

Weiter fehle es nach Auffassung des BVerfG an einer umfassenden Protokollierungspflicht, die eine sachhaltige Prüfung der jeweiligen Überwachungsmaßnahmen ermögliche.[340]

Auch mangele es an einer Berichtspflichten gegenüber Parlament und Öffentlichkeit[341], wie sie nunmehr der nach dem Urteil des BVerfG zur Altfassung des ATDG[342] eingefügte § 9 Abs. 3 ATDG[343] vorsieht, mit einer Berichtspflicht über den Datenbestand und die Nutzung der Antiterrordatei gegenüber dem Bundestag und der Pflicht zur Veröffentlichung über den Internetauftritt des BKA. Derartige Berichtspflichten sieht das POG für einen Teil der Überwachungsmaßnahmen vor, für die Wohnraumüberwachung[344], für die auf Inhalte der Telekommunikation bezogene Datenerhebung[345] und für die Online-Durchsuchung[346], jedoch nicht für andere Überwachungsmaßnahmen und auch nicht gegenüber der Öffentlichkeit.

3.3.2 Datenerhebung durch den verdeckten Einsatz technischer Mittel in oder aus Wohnungen (§ 29 POG)

Nachdem das BVerfG die neue Fassung des § 100c StPO für mit dem Grundgesetz vereinbar erklärt hat,[347] bezeichnete der Verfassungsgerichtshof Rheinland-Pfalz die entsprechende Regelung der Wohnraumüberwachung nach

340 BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/069 und 1 BvR 1140/09, Rn. 267 und BVerfG, NJW 2013, 1499, 1516, Rn. 215, Rn. 219 (und §§ 5 Abs. 4, 9 ATDG, in denen „eine differenzierte und umfassende Protokollierung aller Zugriffe auf die Datenbank“ angeordnet wird).

341 BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/069 und 1 BvR 1140/09, Rn. 143, 268. Kritisch dazu in NVwZ 2016, 839, 841. Zweifelnd an der Berechtigung des Verfassungsgerichts zu derartigen Ableitungen aus der Verfassung, *Durner*, DVBl. 2016, 780, 783.

342 BVerfG, NJW 2013, 1499, 1517, Rn. 221, 222, vgl. auch Begründung des nachfolgenden Änderungsgesetzesentwurfs BT-Drs. 18/1565 S. 20.

343 Eingefügt mit Änderungsgesetz zum ATDG vom 18.12.2014 (BGBl 2014 I 2318).

344 § 29 Abs. 8 S. 1 POG.

345 § 31 Abs. 7 S. 2 POG iVm § 29 Abs. 8 S. 1 POG.

346 § 31c Abs. 6 POG iVm § 29 Abs. 8 S. 1 POG.

347 Vgl. BVerfG NJW 2007, 2753.

§ 29 POG in der Fassung vom 25.07.2005 als verfassungskonform.[348] Dies haben auch das BVerfG und der BGH für § 29 Abs. 1 POG so gesehen.[349] Demgegenüber steht die Entscheidung des ThürVerfGH zu der entsprechenden thüringischen Landesnorm.[350]

3.3.2.1 Kontakt- und Begleitpersonen als Adressaten

Personenbezogene Daten von Kontakt- und Begleitpersonen dürfen nach dem Gesetzeswortlaut unter den Voraussetzungen des § 26 Abs. 3 S. 1 POG erhoben werden. Der Begriff der Kontakt- und Begleitpersonen, der in § 26 Abs. 3 S. 2 POG näher erläutert ist, genügt nach Ansicht des VerfGH Rh-Pf. den Anforderungen an das verfassungsrechtliche Bestimmtheitsgebot.[351] Da die Voraussetzungen auch insoweit an eine dringende Gefahr für die öffentliche Sicherheit und zusätzlich an eine besonders schwere Straftat anknüpfen, können sich die Betroffenen ausreichend auf eine mögliche Wohnraumüberwachung einstellen.[352] Die gesetzliche Ermächtigung gewährleistet für den VerfGH Rh-Pf. eine durch eine hinreichende Tatsachenbasis belegte Nähebeziehung des durch die Anordnung einer Wohnraumüberwachung Betroffenen zu der damit verbundenen Rechtsgutverletzung.[353] Der Grundrechtsschutz der von einer Wohnraumüberwachung betroffenen Kontakt- und Begleitperson wird für den VerfGH Rh-Pf. nachhaltig dadurch bekräftigt, dass die Wohnraumüberwachung sowohl der Verhinderung einer besonders schweren Straftat, die sogar den Anforderungen des Art. 13 Abs. 3 GG genüge, wie auch der Abwehr einer dringenden Gefahr für die öffentliche Sicherheit i.S.d. Art. 13

348 Vgl. VerfGH Rh-Pf., NVwZ-RR 2007, 721 ff.

349 Vgl. BVerfG NJW 2012, 907, 911; vgl. auch BGH NJW 2009, 3448, 3452 zu § 29 a.F: beanstandet wurde nur der damals fehlende Kernbereichsschutz; kritisch insoweit *Petri*, in: Lisken/ Denninger, Handbuch, Kap. G, Rn. 242, der der Ansicht ist, die Formulierung „zur Abwehr einer dringlichen Gefahr für die öffentliche Sicherheit, insbesondere einer gemeinen Gefahr oder Lebensgefahr“ könnte zu unbestimmt sein.

350 Vgl. ThürVerfGH, Urt. v. 21.11.2012 – 19/09.

351 Vgl. VerfGH Rh-Pf., NVwZ-RR 2007, 721, 728.

352 Vgl. VerfGH Rh-Pf., NVwZ-RR 2007, 721, 728.

353 VerfGH Rh-Pf., NVwZ-RR 2007, 721, 728.

Abs. 4 GG diene.[354] Die Regelung trifft daher für den VerfGH Rh-Pf. einen angemessenen Ausgleich zwischen den abzuwägenden Rechtsgütern.[355]

Im Jahre 2012 hat das BVerfG die Vorschrift des § 29 Abs. 1 POG ebenfalls für verfassungskonform erachtet[356], und zwar im Hinblick auf eine Überwachungsanordnung gemäß § 29 Abs. 1 S. 1 Nr. 1 und Nr. 2 POG a.F., welche am 14.07.2004 angeordnet, am 14.10.2004 verlängert wurde[357] und Verantwortliche nach §§ 4 und 5 POG und über § 29 Abs. 1 S. 1 Nr. 2 POG a.F. Kontakt- und Begleitpersonen nach § 26 Abs. 3 S. 2 POG erfasste[358].

Infolge der Überlegungen des BVerfG in seinem Urteil zum BKAG aus dem Jahr 2016, in welchem die Angemessenheit der Wohnraumüberwachung gegenüber Kontakt- und Begleitpersonen nach Maßgabe des § 20h Abs. 1 Nr. 1c BKAG verneint wurde[359], kommen allerdings Zweifel an der Verfassungsgemäßheit der Regelung in § 29 Abs. 1 Nr. 2 POG auf. Im Hinblick auf die Angemessenheit von Überwachungsmaßnahmen trennt das BVerfG zwischen zwei Gruppen von Maßnahmen, den Zugriffen auf informationstechnische Systeme und der Überwachung von Wohnräumen auf der einen Seite und sonstigen heimlichen Überwachungsmaßnahmen auf der anderen Seite[360]. Der Zugriff auf informationstechnische Systeme und die Wohnraumüberwachung dürften sich wegen der mit ihnen verbundenen Eingriffsintensität nur gegen die für die Gefahr verantwortliche Zielperson richten und nicht auf weitere Personen ausgedehnt werden. Ausnahmen sind die Konstellationen, dass vermutet werden kann, dass sich die Zielperson in der Wohnung eines Dritten aufhält, oder sie in einem informationstechnischen System eines Dritten ermittlungsrelevante Informationen speichert[361]. Hingegen sei bei anderen heimlichen Überwachungsmaßnahmen die Anordnung auch gegenüber Dritten nicht schlechthin ausgeschlossen[362].

---

354 VerfGH Rh-Pf., NVwZ-RR 2007, 721, 728.

355 VerfGH Rh-Pf., NVwZ-RR 2007, 721, 728.

356 Vgl. BVerfG NJW 2012, 907, 911.

357 Vgl. BGH, Urt. v. 14.8.2009 – 3 StR 552/08, Rn. 20.

358 Vgl. BGH, Urt. v. 14.8.2009 – 3 StR 552/08, Rn. 20.

359 BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09, Rn. 114 ff., 191 ff.

360 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09, Rn. 114-116.

361 BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09, Rn. 115, 193.

362 BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09, Rn. 116.

Das für eine Rechtfertigung einer Überwachung in und aus Wohnungen kritische Ausmaß der Gefahrverantwortlichkeit scheint bei den Kontakt- und Begleitpersonen i.S.d. § 20h Abs. 1 Nr. 1c BKAG und i.S.d. § 29 Abs. 1 Nr. 2 POG vergleichbar und legt eine Übertragung der Argumente aus dem zum BKAG ergangenen Urteil des BVerfG auf das POG nahe. In beiden Normen wird die Gruppe der Kontakt- und Begleitpersonen durch ihren Tatbezug (mithin durch ihre Nähe zur Gefahr) definiert. Im BKAG sind unter der in § 20h Abs. 1 Nr. 1c BKAG genannten Kontakt- und Begleitperson die Fallgruppen des § 20b Abs. 2 Nr. 2 BKAG zu verstehen. [363] Der Bundesgesetzgeber wollte mit den von ihm näher ausgeformten Fallgruppen (Kenntnis der Straftat - § 20b Abs. 2 Nr. 2a BKAG, Vorteilsziehung aus der Verwertung der Straftat - § 20b Abs. 2 Nr. 2b BKAG, Instrumentalisierung bei Begehung der Straftat - § 20b Abs. 2 Nr. 2c BKAG) den Anforderungen des BVerfG – wenngleich im Fall des BVerfG-Urteils vom 20.04.2016 erfolglos – entsprechen, nämlich dass konkrete Tatsachen für einen objektiven Tatbezug, insbesondere für eine Verwicklung in den Hintergrund oder das Umfeld der zu verhütenden Straftaten existieren[364]. Indem der rheinland-pfälzische Gesetzgeber – ebenfalls in dem Bestreben, eine den Anforderungen des BVerfG entsprechende Regelung zu schaffen[365] – in § 26 Abs. 3 S. 2 POG einen objektiven Tatbezug verlangt, nimmt er aber die Fallgruppen auf, deren Tatbezug gerade nicht der vom BVerfG geforderten Gefahrverantwortlichkeit genügt. Daher ist die in § 29 Abs. 1 S. 1 Nr. 2 POG vorgesehene Ermächtigung zu Überwachungsmaßnahmen gegenüber Kontakt- und Begleitpersonen als nicht vereinbar mit Art. 13 Abs. 1, 4 GG einzustufen.

---

363 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09, Rn. 167; *Kugelmann*, BKAGesetz, § 20h, Rn. 4; enger *Schenke*, in: Schenke/ Graulich/ Ruthig, Sicherheitsrecht des Bundes, § 20h Rn. 13, § 20g Rn. 10, der nur § 20b Abs. 2 Nr. 2c BKAG darunter versteht, eventuell versehentlich, da der herangezogene Beleg – die Begründung des Gesetzesentwurfs (BT-Drs. 10/10121, S. 25) – „Kontakt- und Begleitpersonen i.S.v. § 20b Abs. 2 Nr. 2 BKAG“ nennt.

364 Vgl. BVerfG, Beschl. v. 25.4.2001 – 1 BvR 1086/99, Rn. 54, 68, zu §§ 9 Abs. 1 S. 1 Nr. 2 HbgGDVP und § 10 Abs. 1 HbgGDVP i.d.F. 02.05.1991.

365 Vgl. LT-Drs. 14/2287, S. 41 mit dem Verweis auf BVerfG, Beschl. v. 25.4.2001 – 1 BvR 1086/99, Rn. 54, 68, zu §§ 9 Abs. 1 S. 1 Nr. 2 HbgGDVP und § 10 Abs. 1 HbgGDVP i.d.F. 02.05.1991

3.3.2.2 Verweis auf den Straftatenkatalog

Nicht nur die Einbeziehung von Kontakt- und Begleitpersonen in die Wohnraumüberwachung als solche ist verfassungsrechtlicher Kritik ausgesetzt ist, sondern auch die Regelung ihrer Voraussetzungen in § 29 Abs. 1 S. 2, Abs. POG bietet Anlass zu einer Prüfung der Verfassungsgemäßheit. Voraussetzung für die Datenerhebung in oder aus Wohnungen bei Kontakt- und Begleitpersonen ist, dass diese zur Verhinderung von besonders schweren Straftaten nach § 29 Abs. 2 POG erforderlich ist. Durch die Erweiterung des Straftatenkatalogs im Jahre 2011 ist Abs. 2 dem Wortlaut nach mit § 100c Abs. 2 StPO identisch, der vom BVerfG für mit der Verfassung vereinbar erklärt wurde[366]. Dies entspricht den Anforderungen, die sich aus Art. 13 Abs. 3 GG an die Strafverfolgung ergeben. Besonders schwere Straftaten müssen nach Art. 13 Abs. 3 GG im Einzelnen besonders aufgeführt sein und eine Höchststrafe von mehr als fünf Jahren Freiheitsstrafe vorsehen.[367]

Der VerfGH Rh-Pf. sieht in der Regelung einen angemessenen Ausgleich zwischen den abzuwägenden Rechtsgütern.[368] Im Gegensatz dazu hält der ThürVerfGH den Verweis auf einen Straftatenkatalog für unzulässig.[369] Zwar sei es grundsätzlich zulässig, bei der Fassung präventiver Eingriffsbefugnisse auf einzelne Strafrechtsnormen zu verweisen. Allerdings seien zusätzlich bestimmte Voraussetzungen zu beachten, so eine hinreichend bestimmte Gefahrintensität (wie „dringende Gefahr“) und die hinreichende Bestimmung eines Rechtsgüterschutzes. Eine besondere Schwere der Straftat im Einzelfall genüge diesen Anforderungen nicht, da die einzelne Straftat – bevor sie begangen wird – nicht hinreichend absehbar sei.[370] Bei Hochverrat, Völkermord und Mord sei es schwer, auszumachen, welches insoweit eine besonders schwere Tat im Einzelfall darstellen soll. Der Charakter der Gefahrenabwehr als Rechtsgüterschutz verlange, dass bei der Normierung von Grundrechtseingriffen die zu schützenden Rechtsgüter und die Intensität ihrer Gefährdung in den Blick genommen würden. Nur so lasse sich sicherstellen, dass die polizeilichen Befugnisse im Einzelnen gerechtfertigt seien und zu dem erstrebten Erfolg nicht außer Verhältnis stünden. Durch einen Verweis auf einen Straftaten-

366 Vgl. BVerfG NJW 2012, 833, 836.

367 Vgl. BVerfG NJW 2004, 999, 1012.

368 Vgl. VerfGH Rh-Pf., NVwZ-RR 2007, 721, 728.

369 Zum Folgenden vgl. ThürVerfGH, Urt. v. 21.11.2012 – 19/09.

370 Zum Folgenden vgl. ThürVerfGH, Urt. v. 21.11.2012 – 19/09.

katalog gehe dieser Zusammenhang zwischen Grundrechtseingriff und Rechtsgüterschutz weitgehend verloren. Ähnlich argumentierte das BVerfG für den Fall, dass ein Katalog Vorbereitungshandlungen und bloße Rechtsgutsgefährdungen unter Strafe stellt.[371]

Die rechtlichen Ausführungen im Urteil des ThürVerfGH sind jedoch nur bedingt für die Verhältnisse in Rheinland-Pfalz fruchtbar zu machen.

- § 29 POG verweist auf besonders schwere Straftaten. In Thüringen müssen diese darüber hinaus gemäß § 35 Abs. 1, § 31 Abs. 5 ThürPAG auch „im Einzelfall" schwer wiegen.
- In Rheinland-Pfalz muss eine dringende Gefahr für die öffentliche Sicherheit vorliegen. In Thüringen ist eine dringende Gefahr – trotz Art. 13 Abs. 4 GG – nicht vorgeschrieben. Die Formulierung einer dringenden Gefahr genügt auch nach Auffassung des BVerfG den Bestimmtheitsanforderungen.[372] Sie schließt allgemeine Vorsorgemaßnahmen der Polizei aus.

Folgende Ausführungen sind allerdings auch für Rheinland-Pfalz relevant:

Bei einem Verweis auf einen Straftatenkatalog ist für den Gesetzesanwender nicht hinreichend absehbar, ob die Voraussetzungen vorliegen. Dies gilt für qualifizierte Straftaten, wie etwa räuberische Erpressung, welche im Gegensatz zur einfachen Erpressung vom Katalog umfasst ist. Gleiches gilt für die Abgrenzung zwischen Raub und Erpressung. Teilweise wird in Straftatbeständen, auf die verwiesen wird, weiterverwiesen.[373] Die Kritik an der praktischen Handhabbarkeit der Vorschrift wird auch für § 100c StPO erhoben.[374] Hinzu kommt, dass der Straftatenkatalog zwar auch den strafbaren Versuch erfasst, nicht aber Vorbereitungshandlungen, etwa durch eine andere Straftat.[375] Andererseits ist zu bedenken, dass der Gesetzgeber über einen Beurteilungsspielraum verfügt.[376]

---

371 Vgl. BVerfG NJW 2010, 833, 841 zu §§ 113a, 113b TKG.

372 Vgl. BVerfG NJW 2012, 907, 911.

373 Gegen die Anführung von Straftatenkatalogen für den Bereich der Gefahrenabwehr auch *Leipold*, NJW-Spezial 2013, 56, 47.

374 Vgl. *Schmitt*, in: Meyer-Goßner/ Schmitt, StPO, § 100c Rn. 1; *Kötter*, DÖV 2005, 225, 233.

375 Vgl. *Petri*, in: Lisken/ Denninger, Handbuch, Kap. G, Rn. 251.

376 Vgl. BVerfG, Urt. v. 3.3.2004 – 1 BvR 2378-98, Rn. 237.

Das BVerfG wird teilweise dahingehend verstanden, dass Straftatenkataloge in polizeilichen Vorschriften verfassungswidrig seien.[377] Verwiesen wird dabei auf die Entscheidung des BVerfG zur Vorratsdatenspeicherung. Erforderlich sei stattdessen ein unmittelbarer Bezug auf die zu schützenden Rechtsgüter. Die Entscheidung betraf allerdings nur Straftatbestände, soweit sie Vorbereitungshandlungen und bloße Rechtsgutgefährdungen unter Strafe stellen.[378] Daher kann ein Straftatenkatalog wie in § 29 Abs. 1 Nr. 2, Abs. 2 POG als Voraussetzung für eine polizeilich-präventive Überwachung nicht per se als unzulässig angesehen werden.

3.3.2.3 Nichtstörer

Wie die Inanspruchnahme von Kontakt- und Begleitpersonen gemäß § 29 Abs. 1 S. 1 Nr. 2 POG unterliegt auch die in § 29 Abs. 1 S. 1 Nr. 1 POG vorgesehene Inanspruchnahme des Nichtstörers bei der Wohnraumüberwachung vor dem Hintergrund der neueren Rechtsprechung des BVerfG[379] Zweifeln im Hinblick auf die Angemessenheit der Regelung. Der VerfGH Rh-Pf. hat allerdings in seinem Urteil aus dem Jahr 2007 zu dieser Norm nicht nur die Datenerhebung gegenüber Kontakt- und Begleitpersonen, sondern auch die Durchführung einer Wohnraumüberwachung gegen so genannte nicht verantwortliche Personen i.S.d. § 7 Abs. 1 POG für zulässig erachtet[380]. Der VerfGH Rh-Pf argumentiert, dass der Gesetzgeber eine die Angemessenheit der gesetzlichen Ermächtigung noch wahrende Einschränkung getroffen habe, da Maßnahmen gegen die Betreffenden gem. § 7 Abs. 1 Nr. 2 POG erst dann gerichtet werden dürfen, wenn Maßnahmen gegen die nach den § 4 oder § 5 POG Verantwortlichen nicht oder nicht rechtzeitig möglich sind oder keinen Erfolg versprechen, und daher nur in Ausnahmefällen in Betracht zu ziehen sein werden.[381] Dadurch dass das BVerfG den zulässigen Adressatenkreis der Wohnraumüberwachung nunmehr enger als der VerfGH Rh-Pf. zieht und nur auf Gespräche

---

377 Vgl. *Möstl*, DVBl. 2010, 809, 811 f. unter Berufung auf BVerfGE 125, 260 ff. = BVerfG NJW 2010, 833 ff., wobei *Möstl* aber die Auffassung des BVerfG ablehnt; ebenfalls ablehnend *Schenke*, POR, Rn. 197d.

378 Vgl. BVerfG NJW 2010, 833, 841; ebenso auch BVerfG NJW 2004, 2213, 2218.

379 BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09.

380 Vgl. VerfGH Rh-Pf. NVwZ-RR 2007, 721,727.

381 Vgl. VerfGH Rh-Pf. NVwZ-RR 2007, 721,727.

der gefahrverantwortlichen Zielperson gerichtete Maßnahmen für zulässig erachtet, eine Ausdehnung auf weitere Personen dagegen für unzulässig[382], müssten auch Nichtstörer aus dem Adressatenkreis heimlicher Wohnraumüberwachung herausfallen. Nicht beanstandet hat das BVerfG allerdings die Regelung des § 20h Abs. 2 BKAG, welcher die Überwachung als Verhaltens- oder Zustandsstörer verantwortlicher Personen nicht nur in deren eigener Wohnung, sondern auch in der Wohnung Dritter erlaubt, wenn sich die Zielperson dort aufhält und Maßnahmen in der Wohnung der Zielperson allein nicht zur Abwehr der Gefahr führen werden.[383]

3.3.2.4 Vorbereitungs- und Begleitmaßnahmen

Wie bereits erläutert, ist in einigen Bundesländern ausdrücklich die Polizei ermächtigt, die für die Maßnahme erforderlichen Vorbereitungshandlungen zu treffen (→ Kapitel 3.2.2.1, S. 22).[384] Zwar fehlt eine ausdrückliche Regelung in Rheinland-Pfalz. Es ist insoweit allerdings anerkannt, dass notwendige erforderliche Vorfeldmaßnahmen erst recht von § 29 POG erfasst sind.[385] Denn es liegt in der Natur der Sache, dass die technischen Mittel installiert werden müssen.

Fraglich ist aber, ob dies auch für die nachträgliche Entfernung gilt.[386] Thüringen und Hessen ermächtigen die Polizei ausdrücklich dazu, die Wohnung zu betreten, um die technischen Voraussetzungen zu schaffen. Die Entfernung

---

382 BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09, Rn. 115.

383 BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09, Rn. 188; vgl. auch *Bäcker*, BKA, S. 78 f. und BVerfG, NJW 2004, 999, 1012 ff. (zu einer Wohnraumüberwachung nach § 100c Abs. 2 S. 5 StPO aF (der mit § 100c Abs. 3 S. 2 StPO im Wesentlichen übereinstimmt)).

384 Vgl. § 15 Abs. 7 HSOG; § 41 Abs. 2 SächsPolG; § 35 Abs. 3 ThürPAG.

385 Vgl. *Roos/ Lenz*, POG, § 29 Rn. 3; *Beckmann/ Schröder*, PdK, § 29 Rn. 4; *Schmitt*, in: Meyer-Goßner/ Schmitt, StPO, § 100c Rn. 7; *Böhrenz/ Siefken*, Nds. SOG, § 35a Nr. 2; *Hauser*, in: Honnacker u.a., PAG, Art. 34e (aufgehoben) Rn. 18; *Käß*, BayVBl 2010, 1, 13 zu Art. 34e BayPAG a.F.; *Hegmann*, in: Graf, StPO, § 100c Rn. 3.

386 Dafür Landesregierung, LT-Drs. 14/2287 S. 46; *Roos/ Lenz*, POG, § 29 Rn. 3; *Beckmann/ Schröder*, PdK, § 29 Rn. 4; *Bratke*, Quellen-TKÜ, S. 280 f; *Henrichs*, Kriminalistik 2008, 438, 441 zu § 100h StPO; a.A. die H.M.: Berner/ Köhler/ Käß, BayPAG, Art. 34 Rn. 31; *Günther*, in: MüKo StPO, § 100c Rn. 50; vgl. auch BGH NJW 2001, 1658, 1659; LG Hamburg, Beschl. V. 13.09.2010 –. 608 Qs 17/10.

wird davon nicht erfasst.[387] Der BGH spricht von Vorbereitungs- und Begleitmaßnahmen sowie gegebenenfalls Maßnahmen zur technischen Durchführung, die mit dem Abhören typischerweise unerlässlich verbunden sind.[388] Sie dürfen den gesetzlich ausdrücklich zugelassenen Eingriff nicht an Intensität überschreiten.[389] Für eine Annexkompetenz zur nachträglichen Entfernung spricht, dass die Anbringung selbst ebenfalls auf eine Annexkompetenz gestützt werden kann.[390] Zu bedenken sind allerdings Sinn und Zweck derartiger Maßnahmen. Bei der Wohnraumüberwachung nach § 29 POG handelt es sich um ein besonderes Mittel *verdeckter* Datenerhebung. Diese hat nur die intendierte Wirkung, weil eine effektive Gefahrenabwehr bei vorheriger Bekanntgabe der Maßnahme nicht gewährleistet werden könnte. Das Wirken der Polizei oder das Bemerken der Erhebung soll gezielt verhindert werden.[391] Grundsätzlich sind Daten offen zu erheben (vgl. § 26 Abs. 5 POG[392]). Verdeckte Maßnahmen bedürfen daher einer besonderen Rechtfertigung. Wird die Maßnahme beendet, so kann dies mehrere Ursachen haben. Entscheidend ist jedoch, dass der Betroffene grundsätzlich nach § 40 Abs. 5, 6 POG zu unterrichten ist. In diesen Fällen macht es keinen Sinn, die angebrachten technischen Mittel heimlich wieder zu entfernen, gleichzeitig aber den Betroffenen darüber zu informieren, dass die Maßnahme durchgeführt wurde. Etwas anderes gilt jedoch dann, wenn eine Unterrichtung unterbleibt, weil eine Gefahrenlage noch besteht oder sich ein strafrechtliches Ermittlungsverfahren anschließt.

---

387 Vgl. Art. 35 Abs. 3 ThürPAG; Ebert/ Seel, ThürPAG; § 35 Rn. 23; § 15 Abs. 7 HSOG; *Meixner/ Fredrich*, HSOG, § 15 Rn. 19a.

388 Vgl. BGH NJW 1997, 2189; BGH NStZ 2001, 386, 387.

389 Vgl. BGH NStZ 2005, 278.

390 Vgl. *Schneider*, NStZ 1999, 388, 390 zu § 100c StPO a.F.

391 Vgl. *Roos/ Lenz*, POG, § 28 Rn. 1.

392 Vgl. auch Art. 30 Abs. 3 BayPAG; § 19 Abs. 1, 2 PolG BW; § 18 Abs. 2 ASOG Bln; § 29 Abs. 3 BbgPolG; § 27 Abs. 2 BremPolG; § 2 Abs. 3 PolDVG HA; § 13 Abs. 7 HSOG; § 26 Abs. 2 SOG M-V; § 30 Abs. 2 Nds. SOG; § 9 Abs. 4 PolG NRW; § 25 Abs. 3 SpolG; § 36 Abs. 5 SächsPolG; § 15 Abs. 6 SOG LSA; § 178 Abs. 2 LVwG; § 31 Abs. 3 ThürPAG.

3.3.3 Überwachung und Aufzeichnung der Telekommunikation (§ 31 Abs. 1, 2 POG)

In der Vorschrift zur Telekommunikationsüberwachung sowie zur Online-Durchsuchung wird vorausgesetzt, dass die Maßnahme „zur Abwehr" einer (gegenwärtigen) Gefahr durchgeführt wird. Anders als für die Nachrichtenmittler ist für die Inanspruchnahme der Verantwortlichen nach § 31 Abs. 1 Nr. 1 nicht vorgeschrieben, dass **„**bestimmte Tatsachen**"** vorliegen. Die entsprechende Formulierung in § 100a Abs. 1 StPO enthält dagegen das Erfordernis „bestimmter Tatsachen" für alle Adressaten der Überwachungsmaßnahme. Teilweise wird § 31 Abs. 1 POG als hinreichend bestimmt angesehen.[393] Das BVerfG nahm an der Formulierung des § 20l Abs. 1 Nr. 1 BKAG keinen Anstoß, der ebenfalls zur Abwehr einer – wenngleich dringenden – Gefahr die Überwachung der nach § 17 oder § 18 BPolG Verantwortlichen erlaubt.[394] Gegen den mit der Formulierung „wenn dies zur Abwehr einer gegenwärtigen Gefahr für Leib oder Leben unerlässlich ist" definierten Eingriffstatbestand für „Personen, die eine Gefahr nach Absatz 1 verursachen" aus § 17b Abs. 1, Abs. 3 Nr. 1 SOG LSA, hat das VerfG LSA ebenfalls keine Bedenken erhoben.[395]

Die Erstreckung der Telekommunikationsüberwachung- und -aufzeichnung bzw. der Datenerhebung durch Auskünfte (d. h. der Erhebung von Telekommunikationsverkehrsdaten[396]) auf Nachrichtenmittler gemäß § 31 Abs. 1 S. 2 Nr. 2 POG steht mit der Verfassung im Einklang. Die Regelung orientiert sich an den Bestimmungen des § 100a Abs. 3 StPO und § 20l Abs. 1 S. 1 Nr. 3 BKAG.[397] Daher kann die Verfassungsmäßigkeit des § 31 Abs. 1 S. 2 Nr. 2 POG

---

393 Vgl. *Hsieh*, E-Mail-Überwachung, S. 146 f; die Entscheidung des BVerfG, NJW 2005, 2603 ff. zu § 33a Nds. SOG ist dagegen nicht ergiebig, da Abs. 1 S. 1 Nr. 1 der Vorschrift nicht Gegenstand der Entscheidung war.

394 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1140/09, Rn. 231.

395 Vgl. LVerfG LSA, Urt. v. 11.11.2014 – LVG 9/13, Entscheidungsgründe Ziff.2.3.3.1 und Ziff. 2.3.4.1

396 Vgl. LT-Drs. 15/4879, S. 31: „§ 31 (Datenerhebung durch den Einsatz technischer Mittel zur Überwachung und Aufzeichnung der Telekommunikation, Auskunft über die Telekommunikation) Die polizeiliche Ermächtigung zur Überwachung und Aufzeichnung der Telekommunikation sowie zur Erhebung von Verkehrsdaten…"

397 Vgl. LT-Drs. 15/4879, S. 31.

aus den Feststellungen des BVerfG zu § 20l Abs. 1 S. 2 Nr. 3 BKAG[398] (bzw. § 20m Abs. 1 S. 2 Nr. 3 BKAG[399]) gefolgert werden. Das Gericht hält in diesem Urteil die mögliche Erstreckung der Telekommunikationsüberwachung (§§ 20l Abs. 1 Nr. 3 und 4 BKAG) bzw. der Erhebung von Telekommunikationsverkehrsdaten (§ 20m Abs. 1 Nr. 3 und 4 BKAG) auf Nachrichtenmittler bei verfassungskonformer Auslegung für vereinbar mit Art. 10 Abs. 1 GG.[400] Die Norm des § 20l Abs. 1 Nr. 3 und 4 BKAG genüge den Anforderungen des Bestimmtheitsgrundsatzes und erlaube es nicht, Überwachungsmaßnahmen auf alle Personen zu erstrecken, die mit der Zielperson Nachrichten ausgetauscht haben, sondern setzte eigene, in der Anordnung darzulegende Anhaltspunkte dafür voraus, dass der Nachrichtenmittler von der der Zielperson in die Tatdurchführung eingebunden wird und somit eine besondere Tat- oder Gefahrennähe aufweist.[401] Dasselbe gilt für die Erhebung von Telekommunikationsdaten gemäß § 20m Abs. 1 Nr. 3 und 4 BKAG.[402] Ähnlich ist die Argumentation des LVerfG LSA, das in Nachrichtenmittlern i.S.v. § 17b Abs. 3 S. 1 Nr. SOG LSA Personen sieht, die im weiteren Sinne als Störer zu qualifizieren seien.[403]

Dagegen gibt es Gründe, die Telekommunikationsüberwachung bzw. Telekommunikationsverkehrsdatenerhebung gegen Nichtstörer für mit der Verfassung unvereinbar zu halten. Gemäß § 31 Abs. 1 Nr. 1 POG können – anders als bei der Quellen-Telekommunikationsüberwachung gemäß § 31 Abs. 3

---

398 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und BvR 1140/09, Rn. 233 (zu § 20l Abs. 1 Nr. 3 und 4 BKAG) und Rn. 116 allgemein zu heimlichen Überwachungsmaßnahmen.

399 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und BvR 1140/09, Rn. 233, 251 (zu § 20m Abs. 1 Nr. 3 und 4 BKAG) und Rn. 116 allgemein zu heimlichen Überwachungsmaßnahmen.

400 BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und BvR 1140/09, Rn. 233 (zu § 20m Abs. 1 Nr. 3 und 4 BKAG, „Überwachung der Telekommunikation“) und Rn. 251, 233 zu § 20m Abs. 1 Nr. 3 und 4 BKAG, „Erhebung von Telekommunikationsverkehrsdaten […]“).

401 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und BvR 1140/09, Rn. 233 (zu § 20l Abs. 1 Nr. 3 und 4 BKAG) und Rn. 116 allgemein zu heimlichen Überwachungsmaßnahmen.

402 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und BvR 1140/09, Rn. 251, 233 (zu § 20m Abs. 1 Nr. 2 BKAG) und Rn. 116 allgemein zu heimlichen Überwachungsmaßnahmen.

403 LVerfG LSA, Urt. v. 11.11.2014 – LVG 9/13, Entscheidungsgründe Ziff.2.3.4.2 (zu § 17b Abs. 3 S. 1 Nr. 2 SOG LSA).

POG[404] – auch Daten über Nichtstörer i.S.v. § 7 POG erhoben werden. Im Ergebnis gebilligt hat allerdings das LVerfG LSA die in das Fernmeldegeheimnis aus Art. 14 LVerf LSA eingreifende und in § 17b Abs. 1, 2, 3 S. 1 Nr. 3 LSA geregelte Erhebung von Daten über Inhalte und Umstände der Telekommunikation wie auch von Verkehrsdaten von Nichtstörern, so wie letztere in § 10 SOG LSA (einer dem § 7 POG entsprechenden Norm) definiert sind [405]. Die Inanspruchnahme nach § 10 SOG LSA genügt nach Auffassung des LVerfG LSA deswegen noch dem Verhältnismäßigkeitsgrundsatz, weil eine Abwägung, die eine erhebliche eigene Gefährdung und eine Verletzung anderer höherwertiger Pflichten ausschließt, nach § 10 Abs. 1 Nr. 4 SOG LSA (bzw. § 7 Abs. 1 Nr. 4 POG) erfolgt[406]. Auch das Schweizerische Bundesgericht erlaubt die Überwachung Dritter, und dies über den Wortlaut des (dem § 20l Abs. 1 S. 1 Nr. 3 und 4 BKAG im Wesentlichen entsprechenden) Art. 270 lit. b StPO hinaus, und zwar dann, wenn hinreichend konkrete Anhaltspunkte bestehen, dass Dritte von der beschuldigten Person angerufen werden und sich daraus Hinweise auf die Straftat oder den Aufenthaltsort des Anrufers ergeben.[407] Vor dem Hintergrund der Rechtsprechung des BVerfG zum BKAG[408] ist allerdings hinsichtlich der Verfassungsgemäßheit einer gegen Nichtstörer gerichteten Telekommunikationsüberwachung gleichwohl Skepsis angebracht. Wenn das BVerfG bezogen auf die Befugnisse zur Datenerhebung mit besonderen Mitteln des § 20g Abs. 1, 2 BKAG, die weder in das Brief-, Post und Fernmeldegeheimnis aus Art. 10 Abs. 1 GG noch in die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme noch in Art. 13 Abs. 1 GG eingreifen, nicht beanstandet, dass eine Überwachung gemäß § 20 BPolG unter den Voraussetzungen der Notstandspflicht auch gegen den Nichtstörer angeordnet

---

404 Vgl. *Roos/ Lenz*, POG, § 31 POG Rn. 9.

405 LVerfG LSA, Urt. v. 11.11.2014 – LVG 9/13, Entscheidungsgründe Ziff.2.3.4.3.

406 Vgl. LVerfG LSA, Urt. v. 11.11.2014 – LVG 9/13, Entscheidungsgründe Ziff.2.3.4.3 und § 10 Abs. 3 S. 1 Nr. 3 SOG LSA idF v. 27.10.2015.

407 Vgl. BGE 138 IV 232, 238 f. und *Chadoian*, Das Fernmeldegeheimnis im Zeitalter der Internet- und Mobilfunküberwachung, S. 296. Das Szenario ähnelt insoweit der Überwachung des Wohnraums eines Dritten in den Fällen des § 100c Abs. 1 Nr. 3, 4 StPO, in denen die Überwachung der Wohnung eines Dritten erlaubt werden kann, wenn aufgrund bestimmter Tatsachen vermutet werden kann, dass die Zielperson, sich dort zur Zeit der Maßnahme aufhält, sie dort für die Ermittlungen relevante Gespräche führen wird und eine Überwachung ihrer Wohnung allein nicht zur Erforschung ausreicht, vgl. dazu BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1140/09 Rn. 115 mit Verweis auf BVerfGE 109, 279 (353, 355 ff.).

408 BVerf, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1140/09.

werden darf[409], so lässt dies im Wege eines Umkehrschlusses Bedenken entstehen gegen die in § 31 Abs. 1 POG enthaltene und in Art. 10 Abs. 1 GG eingreifende[410] Möglichkeit zur Überwachung von Nichtstörern. Diese Zweifel werden genährt durch die Überlegung, dass die Mitüberwachung Dritter verfassungsrechtlich problematisch ist, weil diese in eine eingriffsintensive staatliche Überwachungsmaßahme geraten bzw. einbezogen werden, obwohl sie kein gefahrerhöhendes Moment begründet haben bzw. ihnen keine Gefahr zurechenbar ist.[411] Im Ergebnis unterliegt die Telekommunikationsüberwachung und ebenso die Erhebung von Telekommunikationsdaten gegen Nichtstörer daher gewichtigen Zweifeln an ihrer Vereinbarkeit mit dem Verfassungsrecht.

Ob bei dem Begriff der Verkehrsdaten die bestimmtheitsrechtlichen Anforderungen eingehalten sind, wird teilweise bezweifelt.[412] Die Bedeutung des Begriffes ist deswegen maßgebend, weil sich nur die Erhebung von Verkehrsdaten auf vergangene Zeiträume erstrecken kann, nicht aber von Inhaltsdaten. Anders als in § 100g StPO und § 20m BKAG wird nicht auf §§ 96, 113a TKG verwiesen. Eine Legaldefinition findet sich zwar in § 3 Nr. 30 BKAG, nicht jedoch im POG. Der Begriff der personenbezogenen Daten ist im subsidiär anwendbaren Landesdatenschutzgesetz definiert (vgl. § 42 POG i.V.m. § 3 Abs. 1 LDSG).

Allerdings findet sich in der Gesetzesbegründung ein Verweis auf §§ 96 Abs. 1 und § 3 Nr. 30 TKG, „wodurch eine Anpassung an den Sprachgebrauch des Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007 (BGBl. I, S. 3198) erfolgt“. [413] Dies ist als ausreichend zur Erfüllung der verfassungsrechtlichen Bestimmtheitsanforderungen anzusehen. Im Wege der systematischen Auslegung von § 31 Abs. 2

---

409 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1140/09, Rn. 159.

410 Vgl. *Roos/ Lenz*, POG § 1, Rn. 1; Rühle, POG, Kap. G, Rn. 100; Ruder Polizeirecht in Baden-Württemberg, Rn. 503(zu § 23a PolG B-W).

411 *Späthe*, Der Ausbau der informatorischen Polizeibefugnisse, S. 298. Allerdings erfasst der Adressatenkreis des dort besprochenen § 33b Abs. 2 S. 1 BbgPolG auch Notstandpflichtige.

412 Vgl. *Petri*, in: Lisken/ Denninger, Handbuch, Kap. G, Rn. 321.

413 Vgl. Landesregierung, LT-Drs. 15/4879, S. 31; *Roos/ Lenz*, POG, § 31 Rn. 3.

und Abs. 6 POG ergibt sich zudem, dass es sich bei um die bei den Diensteanbietern anfallenden und abrufbaren Verkehrsdaten handelt.[414]

Nicht anwendbar ist die Norm des § 31 POG auf beim Provider gespeicherte (gelesene oder ungelesene) E-Mails[415], da während der Speicherung keine Telekommunikation mehr gegeben ist.[416]

3.3.4 Quellen-Telekommunikationsüberwachung (§ 31 Abs. 3 POG)

Rheinland-Pfalz hat in § 31 Abs. 3 POG eine eigene Rechtsgrundlage für eine Quellen-TKÜ vorgesehen[417]. Der hinsichtlich § 100a StPO bestehende Streit, ob eine solche Maßnahme als Annexkompetenz auch auf die Regelung zur Telekommunikationsüberwachung gestützt werden könnte,[418] ist insoweit nicht relevant.

Die nach § 31 Abs. 3 S. 1 POG mögliche Erstreckung der Quellen-Telekommunikationsüberwachung auf Nachrichtenmittler begegnet keinen Bedenken. Das BVerfG hat dies für den Grundtatbestand der Telekommunikationsüberwachung in § 20l Abs. 1 Nr. 2 BKAG gebilligt[419] und damit, in dem es nicht nur

414 Vgl. VerfGH LSA, Urt. v. 11.11.2014 – LVG 9/13, Entscheidungsgründe Ziff. 2.3.3.2 (zu § 17b Abs. 2 SOG LSA) mit Verweis auf § 17b Abs. 2 und 6 SOG LSA, denen § 31 Abs. 2 und Abs. 6 POG entsprechen.

415 Vgl. OVG Koblenz, NJW 2013, 3671, 3672.

416 Vgl. OVG Koblenz, NJW 2013, 3671, 3672; vgl. auch BGH, NJW 2009, 1828 zum Begriff der „Telekommunkation“ im Rahmen des § 100a StPO.

417 Die Gesetzgebungskompetenz für die entsprechende Norm des § 17c SOG LSA (aufgehoben durch § 1 des Gesetzes vom 27. Oktober 2015 (GVBl. LSA S. 559) hat der VerfGH LSA (Urt. v. 11.11.2014, Az. LVG 9/13, Entscheidungsgründe Ziff. 2.4.2 und 2.3.2 bejaht.

418 Vgl. *Henrichs*, Kriminalistik 2008, 438, 442 zu § 31 POG a.F.; zu § 100a StPO: LG Hamburg, MMR 2011, 693, 694; *Petri*, Prüfbericht, S. 59; *Singelnstein*, NStZ 2012, 593, 599; *Schmitt*, in: Meyer-Goßner/ Schmitt, StPO, § 100a Rn. 7a m.w.N; ablehnend *Buermyer*, StV 2013, 476, 477; vgl. Bundesregierung, BT-Drs. 17/11598, S. 5.

419 BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1140/09, Rn. 233.

§ 20l Abs. 1 BKAG, sondern auch § 20l Abs. 2 BKAG an Art. 10 Abs. 1 GG gemessen hat[420], auch für die diesen Grundtatbestand ergänzende Quellen-Telekommunikation[421]. Die einschränkende Auslegung der Zielperson des Nachrichtenmittlers aus § 20l Abs. 1 Nr. 3 (und Nr. 4 BKAG), welche die Anwendung der Norm auf Nachrichtenmittler begrenzt, bei denen (in der Anordnung auszuführende) Anhaltspunkte bestehen, dass sie in die Tatdurchführung eingebunden sind und damit eine besondere Tat- oder Gefahrennähe aufweisen[422], kann daher auch im Rahmen einer Quellen-Telekommunikationsüberwachung für den Nachrichtenmittler, wie er in Anlehnung an § 20l Abs. 1 S. 1 Nr. 3 BKAG in § 31 Abs. 1 S. 1 Nr. 2 POG[423] definiert ist, angewandt werden.

3.3.4.1 Ausschließlich laufende Telekommunikation

Es muss nach Auffassung des BVerfG technisch sichergestellt sein, dass ausschließlich laufende Telekommunikation betroffen ist.[424] Die Quellen-TKÜ wird teilweise für praktisch unanwendbar erachtet. Durch das erforderliche Aufspielen und Abspeichern des Schadprogramms wird in das System eingegriffen und dessen Integrität betroffen.[425] Bereits im Innenausschuss wurde festgestellt, dass an dem überwachten System Veränderungen vorgenommen werden, soweit dies für die Datenerhebung unerlässlich ist.[426] Während dies teilweise für zulässig erachtet wird,[427] ist der Generalbundesanwalt anderer

420 BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1140/09, Rn. 228.

421 § 20l Abs.1 „ergänzt“ als „Grundtatbestand“ die Regelung zur Quellen-TKÜ in § 20l Abs. 2 BKAG, vgl. *Schenke*, in: Schenke/ Graulich/ Ruthig, Sicherheitsrecht des Bundes, § 20l BKAG Rn. 22.

422 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1140/09, Rn. 233 (zu § 20l Abs. 1 Nr. 2 BKAG). Siehe auch schon oben 3.3.3.1.

423 Vgl. LT-Drs. 15/4879, S. 31.

424 BVerfG NJW 2008, 822, 826.

425 Vgl. *Buermeyer/ Bäcker*, HRRS 2009, 433, 439.

426 Vgl. *Globig*, Innenausschuss, 41. Sitzung des Innenausschusses am 04.11.2010, Teil II, S. 15.

427 Vgl. *Hsieh*, E-Mail-Überwachung, S. 56; *Bäcker*, IT-Grundrecht, S. 21 f.

Auffassung[428]. Die technischen Voraussetzungen, die sicherstellen, dass ausschließlich laufende TK betroffen ist, sind nicht vorhanden.[429]

Aus den fehlenden technischen Möglichkeiten, eine Quellen-TKÜ nach § 17c SOG LSA umzusetzen bzw. konkreter aus dem fehlenden Wissen des Gesetzgeber um die Reichweite des Eingriffs, hat das VerfG LSA die Unverhältnismäßigkeit des § 17c SOG LSA[430] hergeleitet[431]. Denn der Gesetzgeber hat nach Auffassung des LVerfG LSA die Polizei zu Maßnahmen und zum Einsatz von (technischen) Instrumenten ermächtigt, die er noch gar nicht kennen und bewerten konnte, weil es sie gar nicht gibt, womit aber eine durch den Gesetzgeber verantwortete Abwägung fehlt, die für eine grundrechtsbeschränkende Maßnahme unverzichtbar ist.[432] Der Gesetzgeber hatte nach Einschätzung des Gerichts nur sehr vage Vorstellungen davon, was technisch möglich ist und welche Abstriche am Schutz von Vertraulichkeit der erhobenen Informationen sowie des Zugriffs auf andere Inhalte, die nicht vom Zweck der Norm erfasst sind, hinzunehmen sind.[433] Ein Problem stellt sich auch bei der nachträglichen Entfernung des Programms. In Bayern war nicht gewährleistet, dass durch den

---

428 Generalbundesanwalt beim Bundesgerichtshof, StV 2013, 476, 477

429 Vgl. zu § 5 Abs. 2 Nr. 11 VSG NRW a.F. BVerfG NJW 2008, 822, 825 f., Rn. 189: „Nach Auskunft der in der mündlichen Verhandlung angehörten sachkundigen Auskunftspersonen kann es im Übrigen dazu kommen, dass im Anschluss an die Infiltration Daten ohne Bezug zur laufenden Telekommunikation erhoben werden, auch wenn dies nicht beabsichtigt ist.“ und BVerfG NJW 2008, 822, 830, Rn. 240… es könne (ferner) nicht ausgeschlossen werden, dass der Zugriff selbst bereits Schäden auf dem Rechner verursacht. So könnten Wechselwirkungen mit dem Betriebssystem zu Datenverlusten führen … Zudem ist zu beachten, dass es einen rein lesenden Zugriff infolge der Infiltration nicht gibt. Sowohl die zugreifende Stelle als auch Dritte, die eventuell das Zugriffsprogramm missbrauchen, können auf Grund der Infiltration des Zugriffsrechners Datenbestände versehentlich oder sogar durch gezielte Manipulationen löschen, verändern oder neu anlegen.“ und auch LVerfG LSA, Urt. v. 11.11.2014 – LVG 9/13, Entscheidungsgründe Ziff.2.3.4 zu der in § 17c SOG LSA a.F. normierten Befugnis zur Erhebung von Telekommunikationsinhalten und –umständen in informationstechnischen Systemen: „Das ergibt sich aus dem in der mündlichen Verhandlung durch die Landesregierung bestätigten Umstand, dass es bislang noch keine technischen Mittel gibt, um die Norm umzusetzen.“ Siehe auch Generalbundesanwalt beim Bundesgerichtshof, StV 2013, 476, 477.

430 Aufgehoben durch § 1 des Gesetzes vom 27. Oktober 2015 (GVBl. LSA S. 559).

431 Vgl. VerfGH LSA, Urt. v. 11.11.2014 – LVG 9/13, Entscheidungsgründe Ziff. 2.4.3.

432 Siehe VerfGH LSA, Urt. v. 11.11.2014 – LVG 9/13, Entscheidungsgründe Ziff. 2.4.3.

433 Siehe VerfGH LSA, Urt. v. 11.11.2014 – LVG 9/13, Entscheidungsgründe Ziff. 2.4.3.

Löschungsvorgang Daten auf dem System verändert werden können.[434] Dagegen ist die Bundesregierung der Ansicht, dass entsprechende Technik bereits vorhanden ist.[435] Das BKA hat eine Fachgruppe eingesetzt, die bis Ende 2014 ein spezielles Programm zur Quellen-TKÜ entwerfen soll.[436]

Allerdings ist – auch nach Auffassung des BVerfG in seiner Beurteilung des § 20l Abs. 2 BKAG[437] – zwischen der Verfassungskonformität einerseits und den technischen Möglichkeiten der Exekutive andererseits zu unterscheiden. Ist es nicht möglich, sicherzustellen, dass ausschließlich Telekommunikation betroffen ist, so ist die Maßnahme nicht anwendbar.[438] Daraus folgt aber nicht die Verfassungswidrigkeit der Norm.[439] Maßgebend ist vielmehr, ob die Vorschrift noch angemessen ist. Der Gesetzgeber hat bei der Frage der Angemessenheit einen *Bewertungs- bzw. Einschätzungsspielraum.*[440] Sachverhalte, die einem schnellen informationstechnischen Wandel unterliegen, können technikoffen formuliert werden.[441]

3.3.4.2 Abgrenzung von § 31 Abs. 3 POG zu § 31c POG

Obwohl sich bei der Quellen-TKÜ und der Online-Durchsuchung die technischen Vorgehensweisen ähneln,[442] ist rechtlich strikt zwischen beiden Maßnahmen zu unterscheiden. In einigen Fällen ist es streitig, ob eine laufende Kommunikation vorliegt oder nicht, und damit auch, ob der Anwendungsbereich des

---

434 Vgl. *Petri*, Prüfbericht, S. 33, wobei etwas anderes gelten soll, wenn die automatische Deinstallation bereits im Programm angelegt ist; ein Antrag auf Änderung der Gesetzes unter Berücksichtigung des Prüfberichts wurde im Plenum abgelehnt, vgl. LT- Drs. 16/14983.

435 Vgl. Bundesregierung, BT-Drs. 17/11598, S. 11.

436 Vgl. Bundesregierung, BT-Drs. 17/11598, S. 7.

437 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/06 und 1 BvR 1140/09, Rn. 234.

438 Vgl. *Bäcker*, IT-Grundrecht, S. 22.

439 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09 Rn. 234 zu § 20l Abs. BKAG; Luch, BRJ 2012, 34, 39.

440 Vgl. *Grzeszick*, in: Maunz/ Dürig, GG, Art. 20 VII. Rn. 120, 122; *Jarass*, in: Jarass/ Pieroth, GG, Art. 20 Rn. 122.

441 *Petri*, in: Lisken/ Denninger, Handbuch, Kap. G, Rn. 49.

442 Vgl. Landesregierung, LT-Drs. 15/4879, S. 32; *Rühle*, POG, Kap. G, Rn. 102; *Petri*, in: Lisken/ Denninger, Handbuch, Kap. G, Rn. 331; *Stadler*, MMR 2012, 18, 20; *Abate*, DuD 2011, 122, 124.

Art. 10 GG eröffnet ist. Nach der Rechtsprechung des BVerfG sind E-Mails während der laufenden Kommunikation und beim Provider von Art. 10 Abs. 1 GG geschützt, auch dann, wenn die E-Mail gelesen und im Online-Speicher abgelegt wurde.[443] Ist die E-Mail außerhalb davon auf dem System des Betroffenen abgespeichert, ist das Fernmeldegeheimnis nicht mehr berührt.[444] Der Schutz des Fernmeldegeheimnisses endet, wenn die Nachricht bei dem Empfänger angekommen und der Übertragungsvorgang beendet ist.[445] Eine andere Ansicht differenziert zwischen Inhaltsverschlüsselung und Transportverschlüsselung. Während die erstere vom Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme umfasst ist und über eine Online-Durchsuchung zugänglich ist, fällt die letztere in den Bereich des Fernmeldegeheimnisses und wäre über eine Quellen-TKÜ zu erreichen.[446] Ein Abgrenzungsproblem ergibt sich, wenn eine E-Mail noch nicht abgesendet wurde, der Absender sie aber dazu bestimmt hat, etwa durch Ablegen in den Versandordner.[447] Diese Abgrenzungsschwierigkeiten stellen die Verfassungsmäßigkeit der einschlägigen Ermächtigungsnormen des POG nicht in Frage.

3.3.4.3 Eignung und Erforderlichkeit

Die Maßnahme ist auch ohne Betretungsrecht der Wohnung geeignet, denn neben der manuellen Installation ist auch die sog. Remote-Installation von Trojanern möglich.[448] Vorschriften in den Länderbestimmungen, die eine gegenwärtige Gefahr voraussetzen, werden teilweise als ungeeignet angesehen.[449] Da die Bestimmung in Rheinland-Pfalz allerdings keine Gegenwärtig-

---

443 Vgl. BVerfG NJW 2009, 2431, 2432 f; *Klesczewski*, in: Säcker, TKG, § 88 Rn. 13; *Schenke*, in: Stern/ Becker, GG, Art. 10 Rn. 48; *Hsieh*, E-Mail-Überwachung, S. 91 f; *Jarass*, in: Jarass/ Pieroth, GG, Art. 10 Rn. 5.

444 Vgl. *Jarass*, in: Jarass/ Pieroth, GG, Art. 10 Rn. 5; *Klesczewski*, in: Säcker, TKG, § 88 Rn. 13; BVerfG NJW 2006, 976, 978.

445 Vgl. BVerfG NJW 2006, 976, 978.

446 Vgl. *Buermeyer*, StV 2013, 470, 474.

447 Vgl. *Schwabenbauer*, AöR 2012, 1, 19; vgl. auch *Hermes*, in: Dreier, GG, Band 1, Art. 10 Rn. 56.

448 Vgl. *Petri*, in: Lisken/ Denninger, Handbuch, Kap. G, Rn. 331.

449 Vgl. *Hornmann*, NVwZ 2010, 292, 295.

keit erfordert, stellt sich dieses Problem insoweit nicht. Eine qualifizierte Gefahr wird in Literatur und vom BVerfG bislang nicht gefordert, ebenso wenig für die Online-Durchsuchung.[450]

Teilweise wird eingewendet, die Quellen-TKÜ sei nicht erforderlich und daher unverhältnismäßig. Ein Zugriff auf die Daten der Internettelefonie direkt beim Anbieter Skype stelle einen verhältnismäßig geringeren Eingriff dar. Das Unternehmen erkläre sich in seinen Bestimmungen bereit, Verkehrs- und Inhaltsdaten nach Aufforderung an die zuständigen Behörden zu übermitteln. Überdies seien sog. Backdoor-Programme vom Betreiber Skype in seinen Programmen eingebaut.[451] Nach Feststellung der Bundesregierung jedoch erklärt sich Skype auf Anordnung nur dazu bereit, Verkehrs- und Bestandsdaten zu erteilen, nicht jedoch Inhaltsdaten.[452] Die Verfassungsmäßigkeit der Norm ist daher nicht berührt.

3.3.5 Mitwirkungspflichten der TK-Diensteanbieter (§ 31 Abs. 6 POG)

Da ohne die Mitwirkung der Diensteanbieter eine TKÜ in der Praxis häufig nicht durchführbar wäre, befasst sich § 31 Abs. 6 ausdrücklich mit den Pflichten, die die Anbieter diesbezüglich treffen. Damit trägt der Landesgesetzgeber der Judikatur des BVerfG Rechnung, wonach – nach dem Bild einer Doppeltür – ausdrücklich nicht nur eine Rechtsgrundlage für die Übermittlung der Daten notwendig ist (wie z.B. im TKG verwirklicht), sondern auch Konterregelungen[453] für deren Abfrage.[454] Bezüglich der Kompetenz des Landesgesetzgebers zum Erlass dieser Regelung ist anerkannt, dass die Befugnis aus Art. 73 Nr. 7 GG des Bundesgesetzgebers zwar die technische Seite des Übermittlungsvorgangs umfasst,[455] die Kompetenzordnung des Grundgesetzes ansonsten aber

450 Vgl. *Globig*, 41. Sitzung des Innenausschusses am 04.11.2010, Teil II, S. 14; *Bratke*, Quellen-TKÜ, S. 132; BVerfG NJW 2008, 822, 826.

451 Vgl. *Stadler*, MMR 2012, 18, 19; *Braun/ Roggenkamp*, K&R 2011, 681, 685; *Luch*, BRJ 2012, 34, 38.

452 Vgl. Bundesregierung vom 21.11.2012, BT-Drs. 17/11598, S. 14.

453 *Bode*, NJ 2005, 5, 6.

454 BVerfG, NJW 2012, 1419,1423.

455 BverfGE 113, 348,368; *Seidl/ Albrecht*, VR 2014, 126, 128.

nicht überlagert wird, so dass die Kompetenz zur Regelung gefahrenabwehrrechtlicher Maßnahmen weiterhin bei den Ländern liegt.[456] Die Gesetzesbegründung führt hierzu zutreffender Weise Folgendes aus: „Die Verpflichtung der Telekommunikationsdienstleister steht mit der Datenerhebung nach Absatz 1 in engem Zusammenhang und ist zum Vollzug des materiellen Inhalts der polizeilichen Befugnis zwingend erforderlich. Insoweit wird die bestehende Kompetenz des Landes zur Abwehr von Gefahren für die öffentliche Sicherheit im Wege der Annexkompetenz auf das Stadium der Durchführung erweitert. Der Landesgesetzgeber kann folglich diese Materie als Annex zum Bereich der Gefahrenabwehr regeln.“[457]

3.3.5.1 Grundrechtliche Implikationen im Hinblick auf die von der Maßnahme Betroffenen

Was die Ermöglichung der Überwachung oder Aufzeichnung anbelangt, stellen sich im Hinblick auf denjenigen, gegen den sich die Überwachungsmaßnahme richtet, aus grundrechtlicher Sicht keine anderen oder weitergehenden Fragen, als dies bei einer alleine durch die Polizei durchgeführten Überwachung der Fall ist; der Diensteanbieter wird lediglich dazu verpflichtet, die Polizei bei der Überwachung zu unterstützen bzw. evtl. auch erst in die Lage zu versetzen, die Überwachung durchzuführen.[458] Damit soll die Polizeiarbeit erleichtert werden, über Abs. 1-3 hinausgehende oder gar eigenständige Eingriffsbefugnisse sind damit nicht verbunden. Insofern kann an dieser Stelle auch die Frage unbeantwortet bleiben, ob Art. 10 GG den privaten Diensteanbieter selbst (unmittelbar oder mittelbar) verpflichtet[459] oder sich alleine an staatliche Stellen richtet[460]. In der fraglichen Konstellation agiert der Private nicht aus Eigeninteresse, sondern wird ausschließlich in staatlichem Auftrag als „Hilfsperson“ tätig, so dass in diesem Fall der gegen staatliche Kenntnisnahme der Telekommunikation gerichtete Schutzzweck des Art. 10 GG zum

---

456 *Schmidbauer*, in: Schmidbauer/ Steiner, BayPAG, Art. 34b Rn. 46; vgl. VerfGH LSA, Urt. v. 11.11.2014 – LVG 9/13, Entscheidungsgründe Ziff. 2.3.2 und 2.3.7 (zu § 17b Abs. 6 SOG LSA).

457 Landesregierung, LT-Drs. 14/2287, S. 48,

458 *Berner/ Köhler/ Käß*, BayPAG, Art. 34b Rn. 4; *Schmidbauer*, in: Schmidbauer/Steiner, BayPAG, Art. 34b Rn. 51.

459 So z.B. *Roos/ Lenz*, POG, § 31 Rn. 1; *Schwabenbauer*, AöR 2012, 1, 23 f. m.w.N.

460 So *Stettner*, in: HdbGR, Band IV, § 92 Rn. 48 ff.

Tragen kommt.[461] Durch die Verpflichtung des privaten Diensteanbieters verändert sich das Schutzniveau für den von der Maßnahme Betroffenen mithin nicht. Entsprechendes gilt für die Verpflichtung der Diensteanbieter, Auskunft über Verkehrsdaten zu erteilen.

3.3.5.2 Grundrechtsschutz der TK-Diensteanbieter

Im Gegensatz zu dem von der TKÜ-Maßnahme Betroffenen, kann sich der Diensteanbieter nicht auf Art. 10 Abs. 1 GG berufen.[462] Grundsätzlich denkbar ist es dagegen, dass die durch Art. 12 Abs. 1 und 14 Abs. 1 GG gewährleisteten Rechte des Diensteanbieters betroffen sind.[463] Dabei ist zunächst zwischen der Indienstnahme als solcher und der Belastung der Diensteanbieter mit den Investitionskosten, die für die Bereitstellung der technischen Anlagen, die die Überwachungsmaßnahmen überhaupt erst ermöglichen, anfallen, zu unterscheiden: Die Indienstnahme als solche muss sich an Art. 12 Abs. 1 S 1 in Verbindung mit Art. 3 Abs. 1 GG messen lassen und wird als verfassungskonform beurteilt;[464] dagegen wird die Verfassungsmäßigkeit der Kostenbelastung der Anbieter kritisch beurteilt,[465] unabhängig davon, ob man neben den genannten Gewährleistungen auch Art. 14 Abs. 1 GG als einschlägig betrachtet[466].

---

461 In anderem Zusammenhang ebenso BVerfGE 107, 209 (313 f.).

462 OLG Zweibrücken, Urt. v. 25.5.2005 – 3 W 63/05, JR 2006, 286, 287; Köhler, JR 2006, 287, 289.

463 OLG Zweibrücken, Urt. v. 25.5.2005 – 3 W 63/05, JR 2006, 286, 287, auch wenn das Gericht zumindest einen „tiefgreifenden Grundrechtseingriff“ verneint.

464 *Kube/ Schütze*, CR 2003, 663, 666, die allerdings auch darauf hinweisemn, dass, sofern bestehende Anlagen verändert werden müssen, auch Art. 14 Abs. 1 GG als Maßstab heranzuziehen ist. So auch *Waechter*, VerwArch 1996, 68, 72 f.; vgl. auch VerfGH LSA, Urt. v. 11.11.2014 – LVG 9/13, Entscheidungsgründe Ziff. 2.3.7., zur zulässigen Beschränkung der Berufsausübungsfreiheit aus Art. 16 Abs. 1 LVerfG LSA durch § 17b Abs. 6 SOG LSA.

465 VG Berlin, Beschl. v. 8.11.2007 – 27 A 315.07 zur Auslandskopfüberwachung; ebenfalls zur Auslandskopfüberwachung *Berger*, CR 2008, 557, 558; *Kube/ Schütze*, CR 2003, 663, 670; vgl. dagegen VerfG LSA, Urt. v. 11.11.2014 – LVG 9/13, Entscheidungsgründe Ziff. 2.3.7., zur zulässigen Beschränkung der Berufsausübungsfreiheit aus Art. 16 Abs. 1 LVerf LSA durch § 17b Abs. 6 SOG LSA. „Die Verhältnismäßigkeit der Regelung ist vor allem auf Grund der in § 17a Abs. 3 SOG LSA verankerten Entschädigungsregelung zu bejahen, auf die § 17b Abs. 6 S .2 SOG LSA verweist.“

466 *Kube/ Schütze*, CR 2003, 663, 667.

Von diesen grundsätzlichen, im TKG geregelten Fragen zu trennen ist die Frage nach der Verfassungsmäßigkeit der Entschädigungsregelung im jeweils konkreten Überwachungsfall. Auch wenn das BVerG im Verfahren zur Vorratsdatenspeicherung selbst gegen die entschädigungslos vorzunehmende Datenspeicherung keine grundlegenden verfassungsrechtlichen Bedenken geäußert hat,[467] wird die Höhe der durch das JVEG, auf die § 31 Abs. 6 S. 4 über § 12 Abs. 5 POG verweist, vorgesehenen Pauschalen durchaus kritisch gewertet.[468] Im Ergebnis werden die Regelungen des JVEG insbesondere angesichts der Ausführungen des BVerfG in der genannten Entscheidung, die die Kostentragungspflicht der Diensteanbieter gewissermaßen als Kehrseite der diesen eingeräumten neuen Gewinnerzielungschancen betrachtet,[469] aber für zumutbar und damit verfassungskonform gehalten.[470]

3.3.5.3 Inhaltliche Reichweite der Verpflichtung

Festzuhalten ist zunächst, dass sich die Auskunftspflicht der Diensteanbieter ausdrücklich nur auf Verkehrsdaten bezieht. Bislang wurden Auskunftsersuchen über Bestandsdaten auf die datenrechtliche Generalklausel des § 26 POG gestützt.[471] Diese Praxis ist nach einem aktuellen Urteil des BVerfG allerdings als verfassungswidrig zu qualifizieren, da das Gericht für den Abruf solcher Daten bei privaten Diensteanbietern eine spezifische fachrechtliche Abrufnorm verlangt. Für den Abruf von Bestandsdaten genügen Rechtsgrundlagen, „die bloß eine schlichte Datenerhebung von frei zugänglichen Informationen erlauben, nicht aber auch selbst eine Auskunftspflicht Dritter begründen (wie etwa § 26 Polizei- und Ordnungsbehördengesetz Rheinland-Pfalz […])“ aber gerade nicht.[472] Damit ist es nach der aktuellen Rechtslage in Rheinland-Pfalz derzeit

---

467 BVerfGE 125, 260, 362.

468 *Berger*, CR 2008, 557, 559; zur Angemessenheit der Höhe der Pauschalen grundsätzlich *Coen*, CR 2013, 217 ff.

469 BVerfG, Urt. v. 2.3.2010 – 1 BvR 256/08, CR 2010, 232, 246 f.

470 *Berner/ Köhler/ Käß*, BayPAG, Art. 34b Rn. 2; *Schmidbauer*, in: Schmidbauer/ Steiner, BayPAG, Art. 34b Rn. 196; vgl. VerfG LSA, Urt. v. 11.11.2014 –. LVG 9/13, Entscheidungsgründe Ziff. 2.3.7 (zu § 17b Abs. 6 und § 17a Abs. 3 SOG LSA).

471 GdP, LT-Drs. 16/3094, S. 2.

472 BVerfG, NJW 2012, 1419, 1427 f., Rn. 167.

nicht möglich, neben Verkehrsdaten auch Bestandsdaten bei den Diensteanbietern zu erheben.[473]

Die grundsätzliche Zulässigkeit des Verlangens von Auskünften über zukünftig erst anfallende Verkehrsdaten spricht trotz des Fehlens einer § 100g Abs. 1 S. 3 StPO vergleichbaren expliziten Anordnung auch für die Zulässigkeit einer Datenerhebung in Echtzeit – gewissermaßen „live“. Allerdings ist an dieser Stelle zu berücksichtigen, dass aufgrund der Verkehrsdaten, insbesondere aufgrund der Standortdaten, quasi automatisch Bewegungsbilder entstehen, sofern die Maßnahme nicht nur ganz punktuell eingesetzt wird.[474] Dies zeigt die erhebliche Grundrechtsrelevanz der angesprochenen Maßnahmen, die sich noch verschärft, wenn die Datenerhebung in Echtzeit erfolgt. Unter dem Aspekt der Normenklarheit wäre es daher wünschenswert, dass die Zulässigkeit derart einschneidender Maßnahmen explizit geregelt wird.

3.3.5.4 Dynamischer Verweis auf Bundesrecht (TKG etc.)

§ 31 Abs. 6 S. 3 POG verweist insofern dynamisch auf das Bundesrecht, als nicht auf eine bestimmte Fassung der genannten Vorschriften verwiesen wird. Damit handelt es sich, auch wenn die Wendung „in der jeweils gültigen Fassung“ fehlt, um einen dynamischen Verweis, ähnlich wie bei Art. 34b Abs. 1 BayPAG. Für diese Vorschrift ist die Verfassungsmäßigkeit der dynamischen Verweisung unbestritten, da der Landesgesetzgeber die grundsätzliche Mitwirkungspflicht selbst geregelt hat und die Verweisung sich lediglich auf die Art und Weise der Mitwirkung des Diensteanbieters sowie die verfahrensmäßige Abwicklung der Unterstützungs- bzw. Auskunftspflicht bezieht. In diesen Fällen ist es unschädlich, wenn der Landesgesetzgeber bei Erlass der Vorschrift noch nicht wissen konnte, wie die in Bezug genommenen, evtl. zukünftig gültigen bundesrechtlichen Regelungen konkret ausgestaltet sein werden.[475]

---

473 So auch GdP, LT-Drs. 16/3094, S. 2; vgl. z.B. auch Bbg LT-Drs. 5/8015, S. 2.

474 *Singelnstein*, NStZ 2012, 593, 601, der im Bereich der Strafverfolgung für die längerfristige Verkehrsdatenerhebung zusätzlich das Vorliegen der Voraussetzungen für eine polizeiliche Oberservation verlangt.

475 *Berner/ Köhler/ Käß*, BayPAG, Art. 34b Rn. 4; *Schmidbauer*, in: Schmidbauer/ Steiner, BayPAG, Art. 34b Rn. 54.

3.3.6 Auskunft über Nutzungsdaten (§ 31b POG)

Im Gegensatz zu den meisten übrigen Bundesländern[476] hat sich Rheinland-Pfalz dazu entschieden, der Polizei auch die Möglichkeit des Zugriffs auf Nutzungsdaten von Telemediendiensten einzuräumen. Selbst auf bundesrechtlicher Ebene stellt diese Ermächtigung eher eine Ausnahme dar, lediglich dem BKA wird durch § 20m Abs. 2 BKAG eine solche Befugnis verliehen.

3.3.6.1 Einschlägige Grundrechte

Was die von dem Auskunftsbegehren Betroffenen anbelangt, steht außer Diskussion, dass in deren Recht auf informationelle Selbstbestimmung, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG[477], eingegriffen wird.[478] Umstritten ist hingegen, ob ein Eingriff in das durch Art. 10 Abs. 1 GG gewährleistete Fernmeldegeheimnis vorliegt. Dies wird teilweise mit der Begründung verneint, dass die Daten nicht im Rahmen des eigentlichen Übertragungsvorgangs erhoben werden.[479] Dem ist allerdings entgegenzuhalten, dass das Fernmeldegeheimnis des Art. 10 Abs. 1 GG gerade nicht nur den Übertragungsvorgang als solchen, sondern auch dessen Umstände schützt.[480] So werden sämtliche speicher- und auswertbaren personenbezogenen Spuren der TK, z.B. bei der Internetnutzung, von Art. 10 erfasst,[481] jedenfalls sofern die zugrunde liegende Kommunikation individuellen Charakter aufweist.[482] Da Nutzungsdaten – im Unterschied

476 Lediglich Baden-Württemberg, Brandenburg und Thüringen sowie Nordrhein-Westfalen und Schleswig-Holstein sehen solche Möglichkeiten grundsätzlich vor, allerdings letztere beide beschränkt auf bestimmte Daten, vgl. die Ausführungen unter Ziff. 3.2.6.

477 Im Folgenden wird ausschließlich auf die aus den genannten Bestimmungen des GG abgeleitete Garantie der informationellen Selbstbestimmung eingegangen. Eine gesonderte Auseinandersetzung mit dem Grundrecht auf Datenschutz, Art. 4a Landesverfassung des Landes Rheinland-Pfalz erfolgt nicht. Aufgrund der Materialien zur Einfügung der genannten Vorschrift ist davon auszugehen, dass sich diese Gewährleistung mit dem von der Rechtsprechung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG entwickelten Grundrecht deckt; vgl. nur Landtag, LT-Drs. 13/5066, S. 44.

478 Landesregierung, LT-Drs. 15/4879, S. 35; Roos/ Lenz, POG, § 31b Rn. 4.

479 Landesregierung, LT-Drs. 15/4879, S. 35; Roos/ Lenz, POG, § 31b Rn. 4.

480 Vgl. hierzu die Ausführungen unter Ziff. 3.3.4.1.

481 BVerfGE 115, 166, 183.

482 *Durner*, in: Maunz/ Dürig, GG, Art. 10 Rn. 86; *Stettner*, in: HdbGR, Bd. IV, § 92, Rn. 55.

zu Bestandsdaten – per definitionem „während und durch die Dienstenutzung notwendigerweise entstehen“[483], kann die Schutzbereichseröffnung des Art. 10 GG nicht mit dem Argument verneint werden, dass die Daten nicht im Rahmen des eigentlichen Übertragungsvorgangs erhoben würden. Auch die Tatsache, dass Nutzungsdaten im Rahmen der Erbringung von nach dem TMG zu beurteilenden Telemediendienstleistungen anfallen und nicht im Rahmen einer TK im Sinne des TKG, führt nicht zwangsläufig zur Verneinung der Schutzbereichseröffnung des Art. 10 GG.[484] Denn ganz grundsätzlich gilt, dass der TK-Begriff des Art. 10 GG eigenständig und nicht deckungsgleich mit dem technischen TK-Begriff des TKG ist.[485]

Ausschlaggebendes Kriterium für die Schutzbereichseröffnung muss – unabhängig von der Frage, ob dabei gleichzeitig eine TK im Sinne des TKG stattfindet – vielmehr sein, ob im jeweiligen Einzelfall konkrete Kommunikationspartner auftreten, die individuell miteinander in Kontakt treten. Dies ist beispielsweise bei einer schlichten Informationsrecherche im Internet zu verneinen.[486] Auch wenn diese Unterscheidung angesichts der aktuellen technischen Entwicklungen zunehmend an Aussagekraft verliert, wird als Indiz für das Vorliegen individueller Kommunikation auf das Vorhandensein von Zugangshindernissen abgestellt.[487] Insofern müsste hier im Einzelfall differenziert werden: Ein Auskunftsersuchen, das sich auf Nutzungsdaten bezieht, die bei Nutzung einer Internetsuchmaschine angefallen sind, wäre demnach „nur“ an Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG zu messen. Demgegenüber dürfte die Nutzung eines Onlineshops als von Art. 10 GG geschützt zu qualifizieren sein.[488]

---

483 Vgl. die Ausführungen unter Ziff. 3.3.5.2.

484 BVerfG, Urt. v. 13.11.2010 – 2 BvR 1124/10, Rn. 13; *Eckhardt*, K&R 2011, 323, 323; *Petri*, in: Lisken/ Denninger, Handbuch, Kapitel G, Rn. 366 geht sogar von einer grundsätzlichen Betroffenheit des Art. 10 GG aus, da Telemediendienste „technisch regelmäßig auf Basis von Telekommunikationsdiensten abgewickelt werden“.

485 *Löffelmann*, AnwBl 2006, 598, 599 m.w.N. in Fn. 29; vgl. auch die Ausführungen unter Ziff. 3.3.3.5 und Ziff.3.3.7.1 ff.

486 *Böckenförde*, JZ 2008, 925, 937; *Durner*, in: Maunz/ Dürig, GG, Art. 10 Rn. 92.

487 *Böckenförde*, JZ 2008, 925, 936 f.; *Durner*, in: Maunz/ Dürig, GG, Art. 10 Rn. 93 f.

488 A.A. *Böckenförde*, JZ 2008, 925, 937: Selbst wenn in diesem Falle eine individualisierte Zugangsberechtigung besteht, fehlt es an einem individuellen Kommunikationspartner, so dass nicht Art. 10 GG, sondern Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG in seiner Ausprägung als Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme einschlägig ist.

Was den Grundrechtsschutz der Telemediendiensteanbieter anbelangt, ist auf die entsprechenden Ausführungen zu § 31 Abs. 6 POG zu verweisen, vgl. Ziff. 3.3.4.2.

3.3.6.2 Maßnahmevoraussetzungen

Wie die Ausführungen zu den einschlägigen Grundrechtsgarantien gezeigt haben, kommt hinsichtlich der von der Maßnahme Betroffenen je nach Fallgestaltung sowohl ein Eingriff in die spezielle Garantie des Art. 10 GG als auch in das Grundrecht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG in Betracht. Allein diese Tatsache spricht dafür, die in § 31b POG niedergelegten Maßnahmevoraussetzungen auch am Maßstab des Art. 10 GG zu messen. Hinzu kommt, dass der Gesetzgeber selbst davon ausgeht, dass die in § 31b POG verbürgte Ermächtigung einen intensiven Grundrechtseingriff darstellt, weil die Daten „weitreichende Rückschlüsse auf die Persönlichkeit der verantwortlichen Person zulassen."[489] Insofern erscheint es nur folgerichtig, wenn sich die Voraussetzungen des § 31b POG „an den übrigen Bestimmungen im Bereich der Telekommunikationseingriffe orientieren."[490]

Soweit sich die Tatbestandsvoraussetzungen und die Beschreibung des von § 31b POG betroffenen Personenkreises mit den entsprechenden Bestimmungen des § 31 Abs. 1 POG decken, kann aufgrund der grundsätzlichen Vergleichbarkeit der Eingriffe auf die dortigen Ausführungen verwiesen werden. U.a. ist auf eine verfassungskonforme Auslegung des § 31b Abs. 1 S. 1 Nr. 2 POG zu achten entsprechend dem Urteil des BVerfG zu § 20m Abs. 1 S. 1 Nr. 3 BKAG, auf dessen Voraussetzungen (der dem § 31b POG entsprechende) § 20m Abs. 2 BKAG verweist[491]. Danach sind in der Anordnung darzulegende Anhaltspunkte dafür erforderlich, dass der Nachrichtenmittler, von der der Zielperson in die Tatdurchführung eingebunden wird und somit eine besondere Tat- oder Gefahrennähe aufweist.[492] Dies gilt auch für die Sätze 2 und 3 des Absatzes 1. Dagegen hat im Bereich des § 31b POG die Erweiterung der

---

489 Landesregierung, LT-Drs. 15/4879, S. 35.

490 *Roos/ Lenz*, POG, § 31b Rn. 4.

491 *Schenke*, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, § 20m BKAG Rn. 18.

492 Vgl. BVerfG, Urt. v. 20.04.2016 –1 BvR 966/09 und 1140/09, Rn. 250, 251, 233 (zu § 20m Abs. 1 Nr. 3 und 4 BKAG).

Auskunftsobjekte auf zukünftig anfallende Nutzungsdaten konstitutive Bedeutung, da die Norm, im Gegensatz zu § 31 POG gerade nicht zu einer Erhebung von Nutzungsdaten ermächtigt.[493] Was die Problematik einer Echtzeit-Datenerhebung anbelangt, ist auf die Ausführungen unter Ziff. 3.3.4.4 zu verweisen.

Auffällig ist, dass § 31b Abs. 1 S. 1 POG – ähnlich wie § 31c Abs. 1 S. 1 POG – nicht verlangt, dass eine gegenwärtige Gefahr vorliegt, mithin auf die zeitliche Nähe der Gefahrenverwirklichung als Kriterium verzichtet. Die Gesetzesbegründung verweist diesbezüglich lediglich auf die Erläuterungen des insoweit wortgleichen § 31c POG. [494] Dort wird der Verzicht auf das Kriterium der zeitlichen Nähe des Gefahreneintritts damit gerechtfertigt, dass „die Maßnahme wegen ihrer technischen Vorbereitungsmaßnahmen regelmäßig nur in den Fällen eingesetzt werden kann, in denen keine zeitlich akute Gefahrensituation vorliegt."[495] Auch wenn diese Begründung im Bereich der Online-Durchsuchung nicht zu beanstanden ist, stellt sich doch die Frage ihrer Übertragbarkeit auf den Bereich der Auskunftsersuchen über Nutzungsdaten. Derartige Auskunftsersuchen sind eher der Erhebung und Auskunft über Verkehrsdaten im Rahmen von TK-Vorgängen vergleichbar. Insbesondere werden in diesen Fällen wohl keine aufwändigen technischen Vorbereitungsmaßnahmen notwendig, so dass die Gesetzesbegründung zu § 31c POG an dieser Stelle nicht übertragbar ist. Auch wenn sich eine explizite Begründung für das Vorliegen einer gegenwärtigen Gefahr im Bereich der TK-Überwachung finden lässt, so ist doch davon auszugehen, dass der Gesetzgeber eingedenk der Hochwertigkeit der in Rede stehenden grundrechtlichen Gewährleistungen möglichst hohe Hürden für einen Eingriff in deren Schutzbereich normieren wollte.

Selbst wenn man die grundsätzliche verfassungsrechtliche Zulässigkeit dieser niedrigeren Eingriffsschwelle nicht in Zweifel zieht,[496] so bleibt es doch zu-

493 Landesregierung, LT-Drs. 15/4879, S. 35.

494 Landesregierung, LT-Drs. 15/4879, S. 35.

495 Landesregierung, LT-Drs. 15/4879, S. 37. Die gleiche Argumentation kann auch für die Quellen-TKÜ, § 31 Abs. 3 POG fruchtbar gemacht werden.

496 Grundsätzlich gilt unter dem Aspekt der Verhältnismäßigkeit eines Grundrechtseingriffs, dass „die Voraussetzungen für die Datenverwendung und deren Umfang in den betreffenden Rechtsgrundlagen umso enger begrenzt werden [muss], je schwerer der in der Speicherung liegende Eingriff wiegt. Anlass, Zweck und Umfang des jeweiligen Eingriffs sowie die entsprechenden Eingriffsschwellen sind dabei durch den Gesetzgeber bereichsspezifisch, präzise und normenklar zu regeln." (BVerfGE 125, 260,

mindest rechtfertigungsbedürftig, warum im Bereich der unter grundrechtlichen Aspekten durchaus vergleichbaren Auskunftsersuchen über Verkehrsdaten im TK-Bereich höhere Anforderungen gestellt werden. Sachliche Gründe sind nicht ersichtlich, insbesondere kann nicht darauf verwiesen werden, die Auskunft über Nutzungsdaten stelle einen weniger schwerwiegenden Grundrechtseingriff dar als die Auskunft über Verkehrsdaten; der Gesetzgeber selbst hat auf die „besondere Grundrechtsintensität der Maßnahmen“ hingewiesen.[497] Dies spricht für eine Anpassung der Eingriffsschwelle nach oben, an die in §§ 31 Abs. 1, 6 oder auch 31e POG normierten Voraussetzungen. Ein solcher Schritt wäre auch aus Gründen der Konsistenz des Gesetzestextes wünschenswert.

3.3.6.3 Sonstige Regelungen

Die Regelung den Telemedienanbietern gegenüber ist der Regelung des § 31 Abs. 6 POG grundsätzlich vergleichbar, lediglich die zu § 31 Abs. 6 S. 2 POG angesprochene Problematik entfällt. Die Verweisung auf § 31 Abs. 4 und 5 POG stellt klar, dass auch die Auskunftserteilung über Nutzungsdaten grundsätzlich nur auf Basis einer richterlichen Anordnung erfolgen darf, und regelt die Zuständigkeit hierfür; auf die entsprechenden Ausführungen kann verwiesen werden.

---

328 mit zahlreichen weiteren Nachweisen). „Im Bereich der Gefahrenabwehr bedeutet dies für den Gesetzgeber, dass er für jede polizeiliche Befugnis die Wahrscheinlichkeit des Gefahreneintritts sowie die Nähe des Betroffenen zur abzuwehrenden Bedrohung klar und bestimmt festzulegen hat“, ThürVGH, Urt. v. 21.11.2012 – 19/09, Rn. 233. Hinsichtlich Rasterfahndung, Online-Durchsuchung und Vorratsdatenspeicherung hat das BVerfG das Vorliegen einer konkreten Gefahr – bei Einhaltung weiterer Kriterien – als Eingriffsvoraussetzung genügen lassen, BVerfG, Urt. v. 04.04.2006 – 1 BvR 518/02, Rn. 133 ff.; BVerfG, NJW 2008, 822, 830 ff.; BVerfGE 125, 260, 330; Trurnit, VBlBW 2011, 458, 460. Da § 31b POG nur bei Vorliegen einer konkreten Gefahr – und nicht anlasslos – zu Auskunftsersuchen ermächtigt, zudem nur zum Schutz besonders hochrangiger Rechtsgüter und nur bezüglich des näher eingegrenzten Personenkreises, ist der Verzicht auf das besondere zeitliche Näheerfordernis des Gefahreneintritts unter verfassungsrechtlichen Aspekten nicht zu beanstanden.

497 Landesregierung, LT-Drs. 15/4879, S. 35.

3.3.7 Datenerhebung durch den Einsatz technischer Mittel in informationstechnischen Systemen (§ 31c POG, sog. Online-Durchsuchung)

3.3.7.1 Allgemeines

Grundlegend für die Beurteilung der Rechtmäßigkeit der Norm ist die Entscheidung des BVerfG zur Online-Durchsuchung.[498] Das Urteil erging zum NWVerfSchG. Das Gericht hat allerdings ausdrücklich klargestellt, dass die von ihm dargelegten Anforderungen für alle Eingriffsermächtigungen mit präventiver Zielsetzung zu beachten sind.[499]

Im Unterschied zur Quellen-TKÜ betrifft die Online-Durchsuchung den Zugriff auf Daten außerhalb einer laufenden Telekommunikation.[500] Die Erhebung kann durch Sichtung, Kopieren, den Einsatz von Keyloggern, von Schadsoftware usw. erfolgen.[501]

3.3.7.2 Das Erfordernis bestimmter Tatsachen

Im Rahmen des Gesetzgebungsprozesses wurden Zweifel an der hinreichenden Bestimmtheit der Vorschrift geltend gemacht. Obgleich § 20k BKAG verlange, dass „*bestimmte Tatsachen* die Annahme rechtfertigen, dass eine Gefahr vorliegt,…“, verlangt § 31c Abs. 1 S. 1 Nr. 2 POG dies nur für die Nachrichtenmittler.[502] Daher hänge die Maßnahme (gegen die Verantwortlichen nach

---

498 Vgl. BVerfG NJW 2008, 822 ff.; kritisch zum Begriff der Online-Untersuchung *Kutscha*, NJW 2007, 1169. Kugelmann, BKA-Gesetz, § 20k Rn. 6, hält die Online-Durchsuchung wegen der fehlenden Möglichkeiten, den effektiven Schutz des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme abzusichern, für verfassungswidrig.

499 Vgl. BVerfG NJW 2008, 822, 832.

500 Vgl. *Rühle*, POG, Kap. G, Rn. 102; *Roos/ Lenz*, POG, § 31c Rn. 1; BVerfG NJW 2008, 822, 826.

501 Vgl. *Roos/ Lenz*, POG, § 31c Rn. 5; *Albrecht/ Dienst*, JurPC 5/2012, Abs. 23; *Abate*, DuD 2011, 122, 125; Landesregierung, LT-Drs. 15/4879, S. 37; kritisch dazu, dass die Möglichkeiten nicht konkret ins Gesetz aufgenommen wurden vgl. *Sandkuhl*, Stellungnahme DAV, S. 10. Gegen eine Aufnahme spricht allerdings, dass die technischen Methoden schnell veralten, vgl. *Kulwicki*, Verfassungswandel, S. 67.

502 Diese Anforderung speziell für Nachrichtenmittler wurde bereits von BVerfG NJW 2003, 1787, 1791 aufgestellt.

Nr. 1) allein von der subjektiven Einschätzung der Polizeibehörde ab.[503] Dagegen spricht, dass § 29 Abs. 1 POG ebenfalls nicht diese Formulierung enthält. Dennoch wurde die Vorschrift vom BVerfG für verfassungskonform erachtet. Die Formulierung entspreche den Anforderungen des Art. 13 Abs. 4 GG.[504] Das Tatbestandsmerkmal der Abwehr lasse die Maßnahme nur noch bei Bestehen einer konkreten Gefahr zu, so der VerfGH Rh-Pf.[505] Für die Aufnahme der bestimmten Tatsachen in die Vorschrift spricht allerdings die Entscheidung des BVerfG zur Online-Durchsuchung. Darin heißt es:

> *„Die gesetzliche Ermächtigungsgrundlage muss weiter als Voraussetzung des heimlichen Zugriffs vorsehen, dass zumindest tatsächliche Anhaltspunkte einer konkreten Gefahr für die hinreichend gewichtigen Schutzgüter der Norm bestehen.“*[506]

An dieser Stelle verweist das BVerfG auf seine Entscheidung zu § 39 AWG a.F. Das BVerfG formuliert dort:

> *„Das Gesetz fordert, dass Tatsachen die Annahme der Planung der jeweiligen Straftaten rechtfertigen. Das Erfordernis des Vorliegens von Tatsachen verdeutlicht, dass bloße Vermutungen nicht ausreichen.“*[507]

In § 39 AWG war teilweise vorgesehen, dass die Maßnahme nur angeordnet werden darf, soweit tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass (...). Dazu führte das BVerfG aus:

> *„Für die in § 39 Abs. 2 S. 1 Nr. 2 und S. 2 AWG vorgesehene Inanspruchnahme eines Dritten genügen Vermutungen oder wenig aussagekräftige tatsächliche Anhalts-punkte nicht. § 39 Abs. 2 S. 2 AWG ist daher nur verfassungsgemäß, wenn auch insofern Tatsachen verlangt werden, die einen hinreichend sicheren Schluss auf die Teilnahme des Verdächtigen am Postverkehr des Dritten oder die Nutzung seines Telekommunikationsanschlusses ermöglichen. Diese*

---

503 Vgl. *Sandkuhl*, Stellungnahme DAV, S. 10.

504 Vgl. BVerfG NJW 2012, 907, 911; vgl. auch BGH NJW 2009, 3448, 3452.

505 Vgl. VerfGH Rh-Pf. NVwZ-RR 2007, 721, 724.

506 Vgl. BVerfG NJW 2008, 822, 831.

507 Vgl. BVerfG NJW 2004, 2213, 2217.

> *Einengung ist durch Auslegung erreichbar, so dass Bestimmtheitsbedenken insoweit nicht durchgreifen."*[508]

In seiner Entscheidung zu Online-Durchsuchung nach Maßgabe des § 20k BKAG verlangt das BVerfG, dass für Eingriffe in das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme tatsächliche Anhaltspunkte für eine im Einzelfall drohende konkrete Gefahr für ein überragend wichtiges Rechtsgut vorliegen[509].

> *„Dem genügt § 20k Abs. 1 BKAG. (…) Auch genügt [die Vorschrift] den verfassungsrechtlichen Anforderungen insoweit, als sie in Satz 1 – in Verbindung mit § 20a Abs. 2 BKAG – auf das Vorliegen bestimmter Tatsachen abstellt, die die Annahme rechtfertigen, dass eine im Einzelfall bestehende Gefahr vorliegt."*[510]

Auch im Rahmen der Absenkung der Gefahrenschwelle in § 20k Abs. 1 S. 2 BKAG auf die Fälle, in denen die Gefahr erst in näherer Zukunft droht, werden dort bestimmte Tatsachen gefordert, die auf eine im Einzelfall durch bestimmte Personen drohende Gefahr hinweisen.

Die Formulierung tatsächlicher Anhaltspunkte genügt somit den Bestimmtheitsanforderungen. § 31c Abs. 1 POG enthält bei Maßnahmen gegen die Verantwortlichen keine derartige Formulierung. Weder das Vorliegen bestimmter Tatsachen noch das tatsächlicher Anhaltspunkte ist vorgeschrieben. Eine verfassungskonforme Auslegung wie bei dem Merkmal der tatsächlichen Anhaltspunkte ist somit nicht möglich.[511] Für das Erfordernis bestimmter Tatsachen spricht auch, dass die Online-Durchsuchung einen intensiven Eingriff in das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme darstellt.[512] Denn nach Ansicht des BVerfG steigt mit der Intensität des

---

508 Vgl. BVerfG NJW 2004, 2213, 2218; vgl. auch *Rachor*, in: Denninger/ Lisken, Handbuch, Kap. E, Rn. 157.

509 BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09, Rn. 212 mit Verweis auf BVerfGE 274, 326, 328 (= NJW 2008, 822, 830 f.)

510 BVerfG, Urt. v. 20.04.2016 – BvR 966/09 und 1 BvR 1140/09, Rn. 212.

511 A.A. *Ziebarth*, Onlinedurchsuchung, S. 220 f.

512 Vgl. BVerfG NJW 2008, 822, 829; BGH NJW 2007, 930, 931; vgl. auch *Schenke*, in: Schenke/ Graulich/ Ruthig, Sicherheitsrecht des Bundes, § 20k BKAG Rn. 5: „Ob durch einen Eingriff in die Vertraulichkeit und Integrität informationstechnischer Systeme zugleich ein Eingriff in den durch Art. 8 EMRK garantierten Schutz der Privatheit ver-

gefährdeten Rechtsguts und der Reichweite das Erfordernis einer hinreichenden Tatsachenbasis.[513] Lediglich die Gesetzesbegründung verweist auf die Rechtsprechung des BVerfG, wonach tatsächliche Anhaltspunkte einer konkreten Gefahr erforderlich seien.[514]

Ein verfassungsrechtlich eindeutiges Ergebnis kann daraus nicht gezogen werden. Der Gesetzgeber kann aber den Bedenken dadurch entgegentreten, dass er die „bestimmten Tatsachen“ in gleicher Weise für § 31c Abs. 1 Nr. 1 und Nr. 2 formuliert.

3.3.7.3 Verantwortliche und Nachrichtenmittler

Die Maßnahme kann gegen Verhaltensverantwortliche durchgeführt werden. Das BVerfG hat auf eine „individuelle Person als Verursacher“ Bezug genommen, ohne eine nähere Unterscheidung zu treffen.[515]

Problematisch ist, dass die Maßnahme sich auch gegen die *Zustandsverantwortlichen* nach § 5 POG richten kann. Zur konkreten Gefahr führt das BVerfG aus:

> *„Die konkrete Gefahr wird durch drei Kriterien bestimmt: den Einzelfall, die zeitliche Nähe des Umschlagens einer Gefahr in einen Schaden und den Bezug auf individuelle Personen als Verursacher.“*[516]

Aus dieser Formulierung wird nach herrschender Auffassung abgeleitet, die Maßnahme dürfe sich nur gegen Verhaltensverantwortliche, nicht aber gegen

---

bunden ist, ist bislang noch nicht entschieden worden, richtigerweise aber zu bejahen. Im Ergebnis leiten sich aus der EMRK aber keine Anforderungen ab, die über das sich aus dem GG ergebende Schutzniveau hinausgehen.“

513 Vgl. BVerfG NJW 2005, 2603, 2610.

514 Vgl. Landesregierung, LT-Drs. 15/4879, S. 36.

515 Vgl. BVerfG NJW 2008, 822, 831; a.A. *Ziebarth*, Onlinedurchsuchung, S. 222, 191, der ohne nähere Erwägungen Aufsichtspersonen und Geschäftsherren nach § 4 Abs. 2, 3 POG aus dem Anwendungsbereich ausscheiden möchte.

516 So BVerfG NJW 2008, 822, 831.

Zustandsverantwortliche richten.[517] Denn sonst könnten auch Inhaber informationstechnischer Systeme, wie etwa Betreiber eines Internet-Servers oder einer Internet-Mailbox, Ziel der Maßnahme sein.[518]

Für diese Überlegung spricht, dass die genannten Betreiber Zustandsverantwortliche sein können. Erforderlich ist nach § 5 POG zumindest die Inhaberschaft der tatsächlichen Gewalt über eine Sache (vgl. §§ 90, 854-856 BGB).[519] Obgleich es sich bei den Daten selbst nicht um Sachen in diesem Sinne handelt, können die Datenträger darunter subsumiert werden.[520] Die Betreiber haben eine gewisse Herrschaftsbeziehung zu den Datenträgern.[521]

Fraglich ist, ob das BVerfG mit seiner oben zitierten Formulierung[522] auch tatsächlich den gefahrenrechtlichen Störerbegriff einschränken wollte.[523] Zum einen stellt es nur auf die Kriterien ab, die für das Vorliegen einer konkreten Gefahr maßgebend sind. Zum anderen wäre dies ein ungewöhnlicher Schritt, da für die übrigen Maßnahmen der verdeckten Datenerhebung wie TKÜ[524] und

---

517 Vgl. *Schneider*, Onlinedurchsuchung, S. 112; *Böckenförde*, JZ 2008, 925, 931; *Gudermann*, Onlinedurchsuchung, S. 249 zu § 20 BKAG; *Drallé*, Vertraulichkeit, S. 121; *Darnstädt*, DVBl. 2011, 263, 268; a.A. Bundesregierung, BT-Drs. 16/10121, S. 30.

518 Vgl. *Baum/ Schantz*, ZRP 2008, 137, 139; *Albrecht/ Dienst*, JurPC 5/2012, Abs. 15; *Gudermann*, Onlinedurchsuchung, S. 249 zu § 20 BKAG.

519 Vgl. *Roos/ Lenz*, POG, § 5 Rn. 2, 11; vgl. auch BT-Drs 16/10121, S. 30:
„Für den Zugriff beim Zustandsstörer im Sinne von § 18 BPolG ist es erforderlich, dass die abzuwehrende Gefahr von der Sache, dem informationstechnischen System, selbst ausgeht."

520 Vgl. *Stresemann*, in: MüKo BGB, § 90 Rn. 25.

521 Vgl. auch *Ziebarth*, Onlinedurchsuchung, S. 191.

522 Vgl. BVerfG NJW 2008, 822, 831

523 *Böckenförde*, JZ 2008, 925, 931 etwa spricht von einem „neuen Gefahrenbegriff".

524 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und BvR 1140/09, Rn. 231 (zu § 20l Abs. 1 Nr. 1 BKAG): „Keinen verfassungsrechtlichen Bedenken unterliegt […] die […] Befugnis zur Überwachung gegenüber den polizeirechtlich Verantwortlichen gemäß § 20l Abs. 1 Nr. 1 BKAG".

Quellen-TKÜ[525] oder die Wohnraumüberwachung in Form eines Lauschangriffs[526] auch Zustandsverantwortliche Adressaten sein können. Zudem hat das BVerfG in seinem BKAG-Urteil die Norm des § 20k BKAG bei verfassungskonformer Auslegung – ohne § 20k Abs. 4 BKAG explizit zu prüfen – hinsichtlich seiner allgemeinen Eingriffsvoraussetzungen mit der Verfassung für vereinbar gehalten[527] und ganz allgemein für Überwachungsmaßnahmen festgestellt, dass (neben Handlungsverantwortlichen) auch Zustandsverantwortliche in besonderer Verantwortung stehen[528]. Im Ergebnis ist daher davon auszugehen, dass Online-Durchsuchungen sich auch gegen Zustandsstörer richten dürfen.

Die Maßnahme gegen den *Nachrichtenmittler* wird teilweise für verfassungswidrig erachtet.[529] Diese Ansicht beruft sich auf dieselbe Stelle im Urteil des BVerfG, wo es heißt:

> *„Die konkrete Gefahr wird durch drei Kriterien bestimmt: den Einzelfall, die zeitliche Nähe des Umschlagens einer Gefahr in einen Schaden und den Bezug auf individuelle Personen als Verursacher."*

Daraus wird abgeleitet, dass andere Personen als der Verursacher nicht als Adressaten der Maßnahme in Betracht kommen. Eine andere Ansicht hält die Maßnahme gegen Nachrichtenmittler für zulässig. Nur so könne vermieden werden, dass die Betroffenen die Maßnahme umgehen.[530] Es gelten teilweise dieselben Einwände wie oben zu den Zustandsverantwortlichen. Unklar ist, ob das BVerfG tatsächlich einen neuen Gefahrenbegriff schaffen wollte oder lediglich auf Kriterien für das Vorliegen einer konkreten Gefahr hingewiesen hat. *Möstl* spricht von einem „konkreten personenbezogenen Gefahrenverdacht",

---

525 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und BvR 1140/09, Rn. 231 (zu § 20l Abs. 1 Nr. 1 BKAG). § 20l Abs.1 „ergänzt" als „Grundtatbestand" die Regelung zur Quellen-TKÜ in § 20l Abs. 2 BKAG, vgl. *Schenke*, in: Schenke/ Graulich/ Ruthig, Sicherheitsrecht des Bundes, § 20l BKAG Rn. 22.

526 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und BvR 1140/09, Rn. 182 (zu § 20h BKAG); LVerfGH Rh-Pf. NVwZ-RR 2007, 721, 728 (zu § 29h Abs. 1S. 1 Nr. 1 POG).

527 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und BvR 1140/09, Rn. 208.

528 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und BvR 1140/09, Rn. 114.

529 Vgl. *Gudermann*, Onlinedurchsuchung, S. 246, 240 zu Art. 34d BayPAG; *Schneider*, Onlinedurchsuchung, S. 112.

530 Vgl. *Käß*, BayVBl. 2010, 1, 9 zu Art. 34d Abs. 1 BayPAG.

Denninger sieht dagegen die Definition insoweit im Rahmen des traditionellen Polizeirechts.[531]

Jedoch spricht gegen die verfassungsrechtliche Zulässigkeit von Online-Durchsuchungen gegen Nachrichtenmittler, dass das BVerfG bei heimlichen Überwachungsmaßnahmen gegen Dritte gestufte Anforderungen stellt[532] bzw. eine deutliche Trennung vornimmt zwischen dem Zugriff auf informationstechnische Systeme in Form einer Online-Durchsuchung[533] und der Überwachung des Wohnraums[534] auf der einen Seite, welche sich unmittelbar nur gegen diejenigen als Zielperson richten dürfen, die für die drohende Gefahr verantwortlich sind[535], da diese Maßnahmen so tief in die Privatsphäre eindringen, dass sie auf weitere Personen nicht ausgedehnt werden dürfen,[536] und auf der anderen Seite den anderen heimlichen Maßnahmen, bei denen eine Anordnung unmittelbar auch gegenüber Dritten nicht ausgeschlossen ist.[537]

Nach hier vertretener Auffassung können daher zwar Zustandsverantwortliche, nicht jedoch Nachrichtenmittler verfassungsrechtlich unbedenklich Adressat der Maßnahme sein.

3.3.7.4 Vorfeldmaßnahmen

Zu den zulässigen Vorfeldmaßnahmen gehört nach Abs. 3 die Erhebung von Daten zur Ermittlung der spezifischen Kennung und des Standortes des Systems. Das Wort „insbesondere“ macht deutlich, dass die Maßnahmen nicht abschließend aufgelistet sind. Dazu dürften neben dem Einsatz von WLAN-

---

531 Vgl. Möstl, DVBl. 2010, 808, 811; Denninger, in: Lisken/ Denninger, Handbuch, Kap. B, Rn. 28.

532 BVerfG, BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und BvR 1140/09, Rn. 114.

533 Vgl. BVerfG NJW 2008, 822, 831 Rn. 251 (zu § 5 Abs. 2 Nr. 11 VSG NRW idF v. 20.12.2006), sowie 833, Rn. 266, 267 (zu § 3 Abs. 1 S. 1 und 2 G 10 idF v. 19.02.2005).

534 Vgl. BVerfG NJW 2004, 999, 1012 (zu einer Wohnraumüberwachung nach § 103c Abs. 3 StPO).

535 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und BvR 1140/09, Rn. 115.

536 BVerfG NJW 2004, 999, 1012 ff.; BVerfG, Urt. V. 20.04.2016 – 1 BvR 966/09 und BvR 1140/09, Rn. 115.

537 Vgl. BVerfG, BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und BvR 1140/09, Rn. 116.

Catchern[538] auch ein Zugreifen über Datenleitungen und die Messung der Geräteabstrahlung gehören.[539]

Das Betreten der Wohnung als Vorfeldmaßnahme kann dagegen nicht auf § 31c POG gestützt werden.[540] Die Online-Durchsuchung allein über das Netzwerk greift nicht in das Wohnungsgrundrecht nach Art. 13 Abs. 1 GG ein.[541] Ein Betretungsrecht für die Wohnung, um entsprechende Vorrichtungen zu regeln, wurde im Innenausschuss diskutiert,[542] aufgrund der Hürden des Art. 13 Abs. 1 GG aber nicht weiter verfolgt.[543] Ob die Vorgaben des Art. 13 Abs. 4, 5 GG zu beachten wären, hat das BVerfG offen gelassen und ist nach wie vor streitig.[544] Eine Annexkompetenz lässt sich aus § 31c POG nicht herleiten. Der Eingriff muss also auf andere Weise erfolgen. In Bayern war zunächst ein Betretungsrecht für Wohnungen in Art. 34e BayPAG vorgesehen, wurde inzwischen aber wieder aufgehoben.[545]

3.3.7.5 Befristung der Maßnahme

Die Befristung der Maßnahme auf höchstens drei Monate ist nach Auffassung des BVerfG verfassungsrechtlich mit der Maßgabe tragfähig, dass es sich hierbei um eine Obergrenze handelt und sich die tatsächliche Dauer der Anordnung nach einer Verhältnismäßigkeitsprüfung im Einzelfall richtet.[546] Das BVerfG selbst ging in seiner Entscheidung „Online-Durchsuchungen“ davon

---

538 Vgl. Landesregierung, LT-Drs. 15/4879, S. 38.

539 Vgl. *Berner/ Köhler/ Käß*, BayPAG, Art. 34d Rn. 4.

540 Vgl. *Soiné*, NVwZ 2012, 1585, 1588; vgl. auch *Roggan*, NJW 2009, 257, 260 zu § 20k BKAG; *Petri*, in: Lisken/ Denninger, Handbuch, Kap. G, Rn. 358 sowie *Schenke*, in: Schenke/ Graulich/ Ruthig, Sicherheitsrecht des Bundes, § 20k BKAG Rn. 3, 15.

541 Vgl. *Böckenförde*, JZ 2008, 925, 926; *Ebert/ Seel*, ThürPAG, § 34a Rn. 66; BVerfG NJW 2008, 822, 826.

542 Vgl. *Pörksen* und *Kugelmann*, 41. Sitzung des Innenausschusses am 04.11.2010, Teil II, S. 20, 27.

543 Vgl. auch BVerfG NJW 2008, 822, 826.

544 Vgl. *Böckenförde*, JZ 2008, 925, 932, dafür *Buermeyer*, RDV 2008, 8, 14; *Kutscha*, NJW 2007, 1169, 1170; *Gudermann*, Onlinedurchsuchung, S. 110.

545 Vgl. *Schmidbauer*, in: Schmidbauer/ Steiner, BayPAG, Art. 34e (aufgehoben) Rn. 1; *Hauser*, in: Honnacker u.a., PAG, Art. 34e (aufgehoben) Rn. 18.

546 BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09, Rn. 216.

aus, dass die Online-Durchsuchung sich über einen „längeren Zeitraum“ erstrecken kann, in dem Änderungen verfolgt werden und die Nutzung des Systems umfassend überwacht wird.[547] Für die Durchführung der Maßnahme wird eine lange Vorbereitungszeit für erforderlich gehalten.[548]

3.3.7.6 Eignung, praktische Anwendung und Verhältnismäßigkeit

Infolge fehlender Ermächtigung für das Betreten der Wohnung ist die Frage der Eignung der Maßnahme zu thematisieren. Es gibt allerdings Möglichkeiten, das System zu infiltrieren, ohne die Wohnung betreten zu müssen. Dazu gehört es, Sicherheitslücken in der installierten Software oder des Herstellers auszunutzen, Schadsoftware bei Downloads des Benutzers oder über E-Mail-Anhänge einzubringen.[549] Deswegen halten einige Autoren eine Wohnungsbetretung nicht für nötig.[550] Eine andere Auffassung hält es für erforderlich, dass die Person des Betroffenen, das informationstechnische System und die Zuordnung des Systems zu der Person bekannt sein müssen, bevor die Maßnahme durchgeführt wird.[551] Bei der Frage der Eignung steht dem Gesetzgeber angesichts des prognostischen Charakters der Entscheidung ein nur begrenzt überprüfbarer *Beurteilungsspielraum* zu.[552] Für eine Eignung spricht, dass durch die Vorfeldbefugnisse nach Abs. 3 die Kennung und der Standort des Systems erfasst werden können. Nach Abs. 5 muss die richterliche Anordnung nur soweit möglich Name und Anschrift enthalten.

Während der Gesetzgeber die Normierung der Vorschrift für erforderlich hielt,[553] wird die praktische Anwendbarkeit der Maßnahme teilweise in Frage gestellt. Zum einen kann sich der Bürger durch Verschlüsselungssoftware

---

547 Vgl. BVerfG NJW 2008, 822, 829; Hoffmann, Vertraulichkeit, S. 115 zu § 20k BKAG.

548 Vgl. *Schmidbauer*, in: Schmidbauer/ Steiner, BayPAG, Art. 34d Rn. 121; Landesregierung, LT-Drs. 15/4879, S. 39, wonach auf eine Regelung zur Gefahr im Verzug gerade wegen des langen Vorlaufs bewusst verzichtet wurde. Vgl. auch *Kugelmann*, BKA-Gesetz, § 20k Rn. 8: „Die Überwachungssoftware darf nicht entdeckt werden. Das Entdeckungsrisiko bewirkt, dass der Trojaner nur sehr punktuell eingesetzt werden kann und der Einsatz einer gewissen Vorlaufzeit bedarf.“

549 Vgl. *Abate*, DuD 2011, 122; *Sieber*, Stellungnahme, S. 6; *Bonin*, Grundrechtsschutz, S. 132.

550 Vgl. *Soiné*, NVwZ 2012, 1585, 1589.

551 Vgl. *Böckenförde*, JZ 2008, 925, 933.

552 Vgl. *Durner*, in: Maunz/ Dürig, GG, Art. 10 Rn. 146.

553 Vgl. Landesregierung, LT-Drs. 15/4879, S. 36.

schützen. Zum anderen erschwert die Auslagerung der Daten auf USB-Sticks oder externe Speicher, die relevanten Daten über eine Person ausfindig zu machen.[554] Allerdings ist dieser Schutz nicht absolut: Wie *Sieber* ausgeführt hat, kann gegen jede Angriffsform eine Abwehrtechnik und gegen jede Abwehrtechnik eine Umgehungsstrategie entwickelt werden.[555]

Das vom Bund und von Bayern verwendete Schadprogramm (sog. Trojaner) wies Funktionen auf, die über eine bloße Quellen-TKÜ bzw. Online-Durchsuchung hinausgehen. Auf die Ausführungen zur Quellen-TKÜ wird verwiesen (→ Kapitel 3.2.4, S. 35 f.). Hat das Programm, das zur Online-Durchsuchung eingesetzt wird, darüber hinaus die Möglichkeit, laufende Kommunikation zu tangieren, so liegt insoweit ein Eingriff vor, der nicht allein durch das Grundrecht auf Vertraulichkeit und Integrität gerechtfertigt werden kann und insoweit unverhältnismäßig ist.[556] Die Polizei müsste sich für einen Eingriff mittels dieser Trojaner sowohl auf § 31 Abs. 3 POG als auch auf § 31c POG berufen, um die Verfassungsanforderungen zu wahren.

Von einer Ungeeignetheit der Maßnahme trotzt fehlendem Betretungsrechts der Wohnung kann daher nicht schlechthin ausgegangen werden.

3.3.8 Funkzellenabfrage (§ 31e POG)

Bei der Funkzellenabfrage handelt es sich um eine Spezialform der Verkehrsdatenerhebung nach § 31 POG.[557] Die Besonderheit der Funkzellenabfrage besteht im Vergleich zu einer „herkömmlichen" Verkehrsdatenauskunft darin, dass die Polizei – da sie weder Rufnummer noch eine sonstige Kennung des zu überwachenden Anschlusses angeben kann – nicht nur Kenntnis von den Verkehrsdaten einer bestimmten Person erhält, sondern von Verkehrsdaten aller Personen, „die in einer bestimmten Funkzelle zur angegebenen Zeit mittels eines Mobiltelefons kommuniziert haben."[558] Da somit potenziell eine große

---

554 Vgl. *Abate*, DuD 2011, 122, 124; *Kutscha*, NJW 2007, 1169, 1171; vgl. auch *Aernecke*, Schutz, S. 111.

555 Vgl. *Sieber*, Stellungnahme, S. 13.

556 Vgl. *Skistims/ Roßnagel*, ZD 2012, 3. 6; *Ziebarth*, Onlinedurchsuchung, S. 49; a.A. *Graf*, in: Graf, StPO, § 100a, Rn. 107g.

557 *Roos/ Lenz*, POG, § 31e Rn. 1; vgl. auch *Schenke*, in Schenke/ Graulich / Ruthig, Sicherheitsrecht des Bundes, § 20m Rn. 28.

558 Landesregierung, LT-Drs. 15/4879, S. 40. *Kugelmann*, BKA-Gesetz, § 20m Rn. 13 spricht von einer „Erleichterung". In Baden-Württemberg erfasst im Gegensatz zu

Anzahl unbeteiligter Dritter von der Maßnahme betroffen wird, kommt ihr aus grundrechtlicher Perspektive besondere Bedeutung zu[559].

Klärungsbedürftig scheint die zeitliche Reichweite der Ermächtigung. Anders als bei § 31 POG fehlt bei § 31e POG eine Aussage darüber, ob die Ermächtigung Auskünfte über bereits angefallene oder zukünftig erst anfallende Verkehrsdaten oder beides umfasst. Zwar wird § 31e POG als Spezialfall der Verkehrsdatenauskunft nach § 31 POG betrachtet, allerdings ist zu berücksichtigen, dass der Gesetzgeber lediglich davon ausging, dass die in § 31 Abs. 1 POG niedergelegten Maßnahmevoraussetzungen auf § 31e POG übertragbar sind.[560] Auch die Tatsache, dass § 31e Abs. 2 auf § 31 Abs. 6 S. 2 Bezug nimmt, wonach auch nach der Anordnung anfallende Verkehrsdaten von der Auskunftspflicht umfasst sind, hilft nur bedingt weiter, da dieser Vorschrift im Rahmen des § 31 rein deklaratorischer Charakter zukommt.[561] Angesichts der wegen der potenziellen Betroffenheit einer Vielzahl von Unbeteiligten gesteigerten Grundrechtsrelevanz der Maßnahme, wäre eine entsprechende Klarstellung wünschenswert.

---

§ 31e POG die dortige Norm des § 23a Abs. 2 S. 6 PolG BW neben der „Telekommunikation“ auch die „Telemediennutzung“.

559 Vgl. BVerfG vom 20.04.2016 – 1 BvR 966/06 und 1 BvR 1140/09 Rn. 252: „Keinen verfassungsrechtlichen Bedenken unterliegt auch § 20m Abs. 3 S. 2 BKAG [= Funkzellenabfrage], der für die Anordnung der Maßnahme Erleichterungen bezüglich der Bezeichnung der zu erhebenden Daten vorsieht;“

560 Ursprünglich sollte § 31e POG folgendermaßen formuliert werden: „Die Polizei kann unter den Voraussetzungen des § 31 Abs. 1 […]“, Landesregierung, LT-Drs. 15/4879, S. 14. Eine Bezugnahme auf § 31 Abs. 2, der sich mit der zeitlichen Komponente der Maßnahmen befasst, war nicht vorgesehen. Durch die wörtliche Widergabe der Eingriffsvoraussetzungen hat sich an dieser Intention nichts geändert, es sollten wegen des Gebots der Normenklarheit lediglich die Eingriffsvoraussetzungen explizit benannt werden, Fraktionen der SPD, CDU und FDP, LT-Drs. 5/5332, S. 3.

561 Vgl. hierzu die Ausführungen unter Ziff. 3.3.4.4.

3.3.8.1 Maßnahmevoraussetzungen

Die Voraussetzungen, unter denen eine Funkzellenabfrage erfolgen darf, entsprechen denen des § 31 POG. Der zunächst geplante bloße Verweis auf § 31 POG[562] wurde aus Gründen der Normenklarheit durch eine textliche Wiedergabe der Eingriffsvoraussetzungen ersetzt.[563] Dies ist zu begrüßen. Demgegenüber ist eine explizite Regelung der Frage, gegen wen sich die Maßnahme richten darf und wer von der Auskunftspflicht betroffen ist, unterblieben. Allerdings lässt sich zumindest die Frage, wer von der Auskunftspflicht betroffen wird, im Wege der Gesetzesauslegung beantworten: Auskunftspflichtig kann nur sein, wer auch tatsächlich Zugriff auf die Funkzellendaten hat, mithin die TK-Anbieter;[564] ob Gleiches auch bezüglich der Frage gelten kann, gegen wen sich die Maßnahme richten darf, erscheint dagegen zweifelhaft. Zwar geht die Gesetzesbegründung davon aus, dass die Maßnahme nur zulässig ist, wenn es darum geht, Verkehrsdaten einer bestimmten „verantwortlichen" Person, die allerdings noch unbekannt ist, zu ermitteln;[565] allerdings hat diese Auffassung keinen Niederschlag im Gesetzestext gefunden, so dass diese Auslegung nicht zwingend ist. Vielmehr enthält § 31e POG keinerlei Konkretisierung des Personenkreises, gegen den die Maßnahme gerichtet werden darf. Selbst wenn man auf den in der Gesetzesbegründung zum Ausdruck kommenden Willen des Gesetzgebers abstellt, fehlen Aussagen dazu, gegen welche „verantwortlichen" Personen die Maßnahme ergriffen werden darf. Unklar bleibt insbesondere, ob hier die allgemeinen Vorschriften der §§ 4, 5, 7 POG eingreifen,[566] oder ob die Spezialregelung des § 31 Abs. 1 POG Anwendung finden soll.[567] Unter dem Aspekt der Normenklarheit und -bestimmtheit wäre eine ausdrückliche Klarstellung wünschenswert.

---

562 Landesregierung, LT-Drs. 15/4879, S. 14.

563 Fraktionen der SPD, CDU und FDP, LT-Drs. 15/5332, S. 3.

564 Der ursprünglich ins Auge gefasste Gesetzestext enthielt eine ausdrückliche Verpflichtung der TK-Anbieter, Landesregierung, LT-Drs. 15/4879, S. 14.

565 Landesregierung, LT-Drs. 15/4879, S. 40.

566 *Roos/ Lenz*, POG, § 31e Rn. 2, was aber in gewissem Widerspruch zur Aussage in Rn. 3 steht.

567 Landesregierung, LT-Drs. 15/4897, S. 40, wobei hier zu berücksichtigen ist, dass sich die Gesetzesbegründung auf die ursprünglich geplante Formulierung des § 31e bezieht, die einen ausdrücklichen Verweis auf § 31 vorsah; *Rühle*, POG, Kap. G Rn. 112; *Roos/ Lenz*, POG, § 31e Rn. 3, was wiederum aber in Widerspruch zur Aussage in Rn. 2 steht.

Die Subsidiaritätsklausel am Ende des Absatzes 1 trägt der besonderen Grundrechtsrelevanz der Maßnahme Rechnung. Dabei dürfte es unschädlich sein, dass der Gesetzgeber auf eine zusätzliche Erwähnung der zwingenden Erforderlichkeit wie in § 31 Abs. 1 POG verzichtet hat. Zum einen handelt es sich bei dieser Vorschrift lediglich um eine Klarstellung,[568] zum anderen folgt bereits aus der allgemeinen Grundrechtsdogmatik, dass bei besonders intensiven Eingriffen in Grundrechte strenge Maßstäbe an die verfassungsrechtliche Verhältnismäßigkeitsprüfung zu legen sind.[569]

3.3.8.2 Verweis auf andere Vorschriften des POG

Die Verweisung des § 31e Abs. 2 POG auf andere Vorschriften des POG erscheint grundsätzlich unproblematisch bzw. kann auf die diesbezüglichen Ausführungen verwiesen werden. Soweit der Verweis allerdings die Vorgaben zur Befristung der Maßnahmen betrifft, § 31 Abs. 4 S. 2 POG, ist angesichts der hohen Intensität des Eingriffs besonderes Augenmerk auf die Verhältnismäßigkeit zu legen. Zwar kann auch diesbezüglich grundsätzlich auf die Ausführungen zu der Parallelregelung des § 31c verwiesen werden,[570] doch stellt sich hier wegen der hohen Anzahl der potenziell von der Maßnahme betroffenen Unbeteiligten die Frage nach der Verhältnismäßigkeit verschärft. Da es sich bei § 31 Abs. 4 S. 2 POG um eine Maximalfrist handelt, dürfte diesen Bedenken aber durch eine regelmäßig kürzere Anordnungsdauer im jeweiligen Einzelfall Rechnung getragen werden können, so dass die Vorschrift nicht zu beanstanden ist[571].

3.3.8.3 Fehlende Inbezugnahme durch § 39a Abs. 3-5 POG

Da es sich bei der Funkzellenabfrage um eine Spezialform der grundsätzlich in § 31 POG geregelten Verkehrsdatenauskünfte handelt, ist auffällig, dass diese Norm, im Gegensatz insbesondere zu §§ 31 und 31b POG, in den Absätzen 3-5 des § 39a POG keine Erwähnung findet. Auch wenn auf den ersten Blick davon auszugehen ist, dass insbesondere der Kenntnisnahme von (TK-)Inhalten

568 *Roos/ Lenz*, POG, § 31e Rn. 2.

569 Vgl. z.B. BVerfG, Beschl. v. 04.04.2006 – 1 BvR 518/02, Rn. 88 – m.w.N.

570 Vgl. die Ausführungen unter Ziff. 3.3.6.

571 BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09, Rn. 251 enthält keine Ausführungen zur Höchstdauer einer Anordnung nach § 20m Abs. 3 S. 1 i.V.m. § 20l Abs. 4 S. 2 BKAG.

ein besonderes Risiko der Tangierung des Kernbereichs privater Lebensgestaltung immanent ist,[572] betont das BVerfG auch die mögliche Kernbereichsrelevanz bloßer Verkehrsdaten:

> *„Auch aus diesen Daten lassen sich jedoch bei umfassender und automatisierter Auswertung bis in die Intimsphäre hineinreichende inhaltliche Rückschlüsse ziehen. Adressaten (deren Zugehörigkeit zu bestimmten Berufsgruppen, Institutionen oder Interessenverbänden oder die von ihnen angebotenen Leistungen), Daten, Uhrzeit und Ort von Telefongesprächen erlauben, wenn sie über einen längeren Zeitraum beobachtet werden, in ihrer Kombination detaillierte Aussagen zu gesellschaftlichen oder politischen Zugehörigkeiten sowie persönlichen Vorlieben, Neigungen und Schwächen derjenigen, deren Verbindungsdaten ausgewertet werden."*[573]

Darüber hinaus ist an dieser Stelle die Wertung des rheinland-pfälzischen Gesetzgebers zu berücksichtigen, der in § 39a Abs. 3 – 5 POG ohne Differenzierung zwischen Inhalts- und Verkehrsdaten auf § 31 POG verweist. Hinzu kommt, dass § 39a Abs. 3 – 5 einen ausdrücklichen Verweis auf § 31b POG enthalten. Begründet wird dies damit, dass die Nutzungsdaten eine der TKÜ und dem verdeckten Zugriff auf informationstechnische Systeme vergleichbare Gefährdungssituationen für den Kernbereich darstellen können,[574] wobei es sich bei Nutzungsdaten im Bereich der Telemedien um das Pendant der im Rahmen einer TK anfallenden Verkehrsdaten handelt und Verkehrsdaten zumindest potenziell kernbereichsrelevant sein können.[575] § 31e POG ermächtigt – im Gegensatz beispielsweise zu § 31a POG – zur Erhebung sämtlicher Verkehrsdaten, die noch dazu einer potenziell sehr großen Anzahl von Nichtstörern zuzuordnen sein dürften. Auch wenn es sich bei der Funkzellenabfrage

---

572 So ausdrücklich mit Bezug auf die akustische Wohnraumüberwachung, die Online-Durchsuchung informationstechnischer Systeme sowie die Inhaltsüberwachung und Auswertung der TK das Dissenzvotum *Schluckebier* zur Vorratsdatenspeicherung, BVerfG, NJW 2010, 833, 852.

573 BVerfG, NJW 2010, 833, 838, Rn. 211. Anders *Schenke*, in: Schenke/ Graulich/ Ruthig, Sicherheitsrecht des Bundes, § 20m BKAG Rn. 7: „Allerdings ist bei der Erhebung von Verkehrsdaten eine Beeinträchtigung des Kernbereichs privater Lebensgestaltung kaum denkbar. Damit konnte der Gesetzgeber auf die Aufnahme von § 20l Abs. 6 entsprechenden Schutzvorschriften verzichten."

574 Landesregierung, LT-Drs. 15/4879, S. 44.

575 BVerfG, NJW 2010, 833, 838; Trurnit, VBlBW 2010, 413, 416; a.A. wohl BGH NJW 2010, 1827, 1829.

regelmäßig um ein eher singuläres Ereignis handeln wird, ist doch zu berücksichtigen, dass auch Funkzellenabfragen theoretisch systematisch durchgeführt werden können und sich so Bewegungsprofile erstellen lassen, die spätestens nach Auswertung der Ergebnisse der Funkzellenabfrage, die zu einer Identifizierung der Zielperson geführt hat, auch individuellen Charakter gewinnen. Angesichts der im Hinblick auf die Gefährdung des Kernbereichs vergleichbaren Situation bei Funkzellenabfrage und „normaler" Verkehrsdaten- bzw. auch Nutzungsdatenerhebung ist nicht ersichtlich, warum § 31e POG im Hinblick auf den Kernbereichsschutz nicht ebenso behandelt wird wie § 31 POG oder wie der im Bereich der Telemedien vergleichbare § 31b POG. Allerdings enthält auch § 20m BKAG keine den Kernbereich privater Lebensgestaltung schützende Vorschriften, ohne dass das BVerfG dies bemängelt hat[576].

3.3.9 Besondere Formen des Datenabgleichs (§ 38 POG, sog. Rasterfahndung)

Bei der Rasterfahndung handelt es sich nach dem BVerfG um „eine besondere polizeiliche Fahndungsmethode unter Nutzung der elektronischen Datenverarbeitung. Die Polizeibehörde lässt sich von anderen öffentlichen oder privaten Stellen personenbezogene Daten übermitteln, um einen automatisierten Abgleich (Rasterung) mit anderen Daten vorzunehmen. Durch den Abgleich soll diejenige Schnittmenge von Personen ermittelt werden, auf welche bestimmte, vorab festgelegte und für die weiteren Ermittlungen als bedeutsam angesehene Merkmale zutreffen."[577]

Unter praktischen Gesichtspunkten wird auf den relativ begrenzten bis nicht vorhandenen Anwendungsbereich der rein präventiven Rasterfahndung hingewiesen.[578] Für das BVerfG dient dieses Instrument der Verdachts- oder Verdächtigengewinnung;[579] ihr Einsatz ist insofern hauptsächlich als Vorfeld-

576 Vgl. BVerfG v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09, Rn. 247-252.

577 BVerfG, Beschl. v. 04.04.2006 – 1 BvR 518/02, Rn. 1.

578 BVerfG, Urt. v. 04.04.2006 – BvR 518/02, Rn. 184 – Sondervotum Haas; *Bausback*, NJW 2006, 1922, 1923; *Schewe*, NVwZ 2007, 174, 176; *Volkmann*, JZ 2006, 918, 920; *ders.,* JURA 2007, 132, 137.

579 BVerfG, Beschl. v. 04.04.2006 – BvR 518/02, Rn. 119.

maßnahme denkbar, was aber angesichts der Schwere der damit verbundenen Grundrechtseingriffe verfassungsrechtlich nicht zulässig ist.[580] Sobald bereits eine Gefahrenlage besteht, wird die Rasterfahndung wegen des mit ihr verbundenen (Zeit-)Aufwandes regelmäßig zu spät kommen.[581] Teilweise wird auch angenommen, dass aufgrund der vom BVerfG aufgestellten Anforderungen an die Konkretheit der Gefahr häufig die Schwelle zum Anfangsverdacht überschritten sein wird, so dass ausschließlich repressive Maßnahmen ergriffen werden können.[582] Dennoch geht das BVerfG weiterhin von der Eignung der präventiven Rasterfahndung [583] und auch von der Verfassungsmäßigkeit der Eingriffsvoraussetzungen und verfahrensrechtlichen Ausgestaltung der Rasterfahndung in § 20j BKAG[584] aus, so dass eine Berechtigung des Instruments zumindest nicht vollständig in Abrede gestellt werden kann.

3.3.9.1 Recht auf Informationelle Selbstbestimmung (Art. 2 i.V.m. 1 GG)

Grundsätzlich wird ein Eingriff in das Recht auf informationelle Selbstbestimmung durch die Rasterfahndung bejaht, sofern Daten nicht nur „ungezielt und allein technikbedingt zunächst miterfasst, aber unmittelbar nach der Erfassung technisch wieder anonym, spurenlos und ohne Erkenntnisinteresse für die Behörden ausgesondert werden."[585] Dabei stellen sowohl die Übermittlungsanordnung, als auch die Speicherung sowie der Datenabgleich Eingriffe

580 BVerfG, Beschl. v. 04.04.2006 – 1 BvR 518/02, Rn. 138 ff.

581 BVerfG, Beschl. v. 04.04.2006 – 1 BvR 518/02, Rn. 143.

582 *Roos/ Lenz*, POG, § 38 Rn. 6.

583 BVerfG, Beschl. v. 04.04.2006 – 1 BvR 518/02, Rn. 84; an dieser Einschätzung ändert auch die Feststellung der Richter nichts, dass die präventive Rasterfahndung, so sie den verfassungsrechtlichen Anforderungen genügt, „in den meisten Fällen zu spät kommen wird, um noch wirksam zu sein", BVerfG, aaO, Rn. 143; Petri in: Lisken/ Denninger, Handbuch, Kapitel G, Rn. 42.

584 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09, Rn. 206, 207.

585 BVerfG, Beschl. v. 04.04.2006 – 1 BvR 518/02, Rn. 74; Urt. v. 14.07.1999 – 1 BvR 2226/94 u.a. , Rn.; 107, 299 (328); Frenz, DVBl. 2009, 333, 335.

dar,[586] denen wegen „der inhaltlichen Weite der Befugnis sowie der mit ihr eröffneten Möglichkeit der Verknüpfung von Daten“ erhebliches Gewicht zukommt.[587]

3.3.9.2 Maßnahmevoraussetzungen

Die Voraussetzungen, unter denen eine Rasterfahndung durchgeführt werden darf, waren in Rheinland-Pfalz häufiger Gegenstand von Änderungen. Nach § 25d a.F. POG konnte lediglich „zur Abwehr einer gegenwärtigen erheblichen Gefahr die Übermittlung von personenbezogenen Informationen oder Informationsbeständen bestimmter Personengruppen auch zum Zwecke des Abgleichs mit anderen Informationsbeständen“ verlangt werden, wenn zusätzlich „tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass dies zur Abwehr der Gefahr erforderlich ist.“ Diese für die polizeiliche Praxis hohe Eingriffsschwelle wurde unter dem Eindruck der Anschläge vom 11.9.2001 deutlich abgesenkt.[588] Ab dem Jahre 2004 durfte die Übermittlung personenbezogener Daten verlangt werden, „soweit dies zur Abwehr einer erheblichen Gefahr oder zur vorbeugenden Bekämpfung von besonders schwerwiegenden Straftaten (§ 29 Abs. 2) erforderlich ist“, § 38 POG a.F. Das BVerfG-Urteil aus dem Jahre 2006 zur Rasterfahndung veranlasste den rheinland-pfälzischen Gesetzgeber sodann ein weiteres Mal, die Eingriffsschwellen für die Rasterfahndung neu zu definieren.[589] Seit 2011 ist sie nach § 38 Abs. 1 POG zulässig „zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person“.

Was die Schutzgüter anbelangt, entspricht die Formulierung der vom Bundesverfassungsgericht geprüften Vorschrift, die diesbezüglich unbeanstandet

---

586 BVerfG, Beschl. v. 04.04.2006 – 1 BvR 518/02, Rn. 74 ff.; *Petri,* in: Lisken/ Denninger, Handbuch, Kapitel G, Rn. 532 m.w.N.

587 BVerfG, Beschl. v. 04.04.2006 – 1 BvR 518/02, Rn. 96 ff., zudem seien die möglichen weiteren Folgen, die Heimlichkeit der Maßnahme sowie die Tatsache, dass es sich um einen verdachtslosen Grundrechtseingriff mit erheblicher Streubreite handele, zu berücksichtigen; *Petri*, in: Lisken/ Denninger, Handbuch, Kapitel G, Rn. 531 mwN; *Achelpöhler/ Niehaus*, DÖV 2003, 49, 50; *Robrecht*, SächsVBl. 2007, 80, 85. Kritisch *Volkmann*, JURA 2007, 132, 134; a.A. z.B. BVerfG, Beschl. v. 04.04.2006 – 1 BvR 518/02, Rn. 169 ff. – Dissenzvotum Haas; OVG Koblenz, NVwZ 2002; 1528, 1529; *Bausback*, NJW 2006, 1922, 1923 f.; *Horn*, DÖV 2003, 746, 748 ff. m.w.N.; *Schenke*, DVBl. 1996, 1393, 1400.

588 Landesregierung, LT-Drs. 14/2287, S. 51.

589 Landesregierung, LT-Drs. 15/4879, S. 42.

geblieben ist, da die genannten Schutzgüter nach Ansicht des BVerfG als „hochwertig“ [590] oder im Fall des § 20j Abs. 1 S. 1 BKAG als „hinreichend gewichtig“[591] zu bezeichnen sind.

Unter Verhältnismäßigkeitsaspekten legte das BVerfG bezüglich der Eingriffsschwelle die hinreichend konkrete Gefahr als Untergrenze fest.[592] Demnach „darf eine Rasterfahndung nicht schon im Vorfeld einer konkreten Gefahr ermöglicht werden, denn sie würde zu vollständig verdachtslos und mit hoher Streubreite erfolgenden Grundrechtseingriffen führen, die Informationen mit intensivem Persönlichkeitsbezug erfassen können.“[593] Andererseits stellte das BVerfG auch klar, dass es aus verfassungsrechtlicher Perspektive nicht erforderlich ist, eine gegenwärtige Gefahr als Eingriffsvoraussetzung zu verlangen.[594] In einer Entscheidung über die Norm des § 20j Abs. 1 S. 1 Halbs. 2 BKAG ließ es die exemplarische Konkretisierung einer Gefahrenlage dergestalt ausreichen, dass „konkrete Vorbereitungshandlungen die Annahme rechtfertigen“, dass vom Gesetz näher bestimmte Straftaten begangen werden[595].

Zwar spricht § 38 Abs. 1 POG „nur“ von einer „Gefahr“ und nicht von einer „konkreten Gefahr“, dennoch ist aber davon auszugehen, dass der Gesetzgeber intentionsgemäß[596] den Vorgaben des BVerfG zur erforderlichen Eingriffsschwelle Rechnung getragen hat. Dem BVerfG ging es in erster Linie darum, die Zulässigkeit der Rasterfahndung im Bereich der Gefahrenvorsorge als unverhältnismäßig zu qualifizieren; dies ist durch die Anknüpfung an den Gefahrenbegriff in Rheinland-Pfalz geschehen. Für die Rechtspraxis muss zudem im Einklang mit dem BVerfG verlangt werden, dass sie diesen Gefahrenbegriff nicht erweiternd im Sinne einer Vorfeldbefugnis auslegt.[597]

---

590 BVerfG, Beschl. v. 04.04.2006 – 1 BvR 518/02, Rn. 91.

591 BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09, Rn. 207.

592 BVerfG, Beschl. v. 04.04.2006 – 1 BvR 518/02, Rn. 125, 133; a.A. *Horn*, DÖV 2003, 746, 750 f.; Zur grundsätzlichen Kritik an der Heranziehung des Gefahrenbegriffs im Bereich rein informationeller Befugnisse *Möstl*, DVBl. 2007, 581, 583 ff., insbesondere 587 f.

593 BVerfG, Beschl. v. 04.04.2006 – 1 BvR 518/02, Rn. 138.

594 BVerfG, Beschl. v. 04.04.2006 – 1 BvR 518/02, Rn. 143; a.A. *Achelpöhler/ Niehaus*, DÖV 2003, 49, 52.

595 BVerfG, Urt. v. 20.04.2016 – Az 1 BvR 966/09 und 1 BvR 1140/09, Rn. 207.

596 Landesregierung, LT-Drs. 15/4879, S. 42.

597 BVerfG, Beschl. v. 04.04.2006 – 1 BvR 518/0, Rn. 154 ff.; so auch Landesregierung, LT-Drs. 15/4879, S. 42.

Auch im Übrigen wurde die zur Überprüfung gestellte, diesbezüglich annähernd wortgleiche nordrhein-westfälische Vorschrift zur Rasterfahndung vom BVerfG nicht beanstandet. Insbesondere entspreche sie dem rechtsstaatlichen Gebot der Normenbestimmtheit und Normenklarheit.[598] Auch die Norm des § 20j BKAG, deren Tatbestand weitgehend dem des § 38 POG entspricht, ist nach Auffassung des BVerfG hinsichtlich ihrer Eingriffsvoraussetzungen hinreichend bestimmt und verhältnismäßig ausgestaltet[599].

3.3.9.3 Bestimmung der zu übermittelnden Daten

Unter dem Aspekt der Normenbestimmtheit und -klarheit, ist es nach Auffassung des BVerfG auch nicht zu beanstanden, dass nicht alle zu übermittelnden Datentypen explizit benannt werden, sondern es der Gesetzgeber der Exekutive ermöglicht, im Einzelfall zu bestimmen, welche weiteren Daten benötigt werden und deren Übermittlung zu verlangen.[600] Die Bestimmtheitsanforderungen seien insofern gewahrt, als der Begriff der überprüften Regelung (andere für den Einzelfall benötigte Daten) „unter Berücksichtigung des Normzwecks der Gefahrenabwehr und damit auch hinsichtlich der Feststellung, wozu die Daten „benötigt“ werden, so konkretisiert werden kann, dass der Verhältnismäßigkeitsgrundsatz gewahrt bleibt.“

Im Gegensatz zur überprüften nordrhein-westfälischen Regelung bezieht sich § 38 Abs. 2 S. 1 POG aber nicht auf im Einzelfall „benötigte“ Daten, sondern ermöglicht es den Ermittlungsbehörden lediglich, im Einzelfall weitere Datenmerkmale festzulegen, die sodann zu übermitteln sind. Allerdings ist auch hier nach Sinn und Zweck der Ermächtigung davon auszugehen, dass die Polizei damit lediglich zur Festlegung solcher Merkmale ermächtigt wird, die sie auch „benötigt“. Diese Auslegung wird auch durch die Gesetzesbegründung gestützt. Dort heißt es: „Die weiteren im Einzelfall festzulegenden Merk-

598 BVerfG, Beschl. v. 04.04.2006 – 1 BvR 518/02, Rn. 150 ff.

599 Vgl. BVerfG, Urt. v. 20.04.2016 – Az 1 BvR 966/09 und 1 BvR 1140/09, Rn. 207.

600 Konkret spricht § 38 Abs. 2 S. 1 POG davon, dass die Übermittlung grundsätzlich auf explizit benannte Daten „sowie auf im Einzelfall festzulegende Merkmale“ zu beschränken ist. Die vom BVerfG überprüfte nordrhein-westfälische Regelung formulierte ganz ähnlich: „Das Übermittlungsersuchen ist auf Namen, Anschrift, Tag und Ort der Geburt sowie andere für den Einzelfall benötigte Daten zu beschränken“.

male richten sich nach dem Fahndungszweck und danach, nach welcher Personengruppe gefahndet wird."[601] Insofern können die Feststellungen des BVerfG zur nordrhein-westfälischen Regelung auf die Rechtslage in Rheinland-Pfalz übertragen werden.

3.3.9.4 Verfahrensbezogene Regelungen

Die Anordnung einer Rasterfahndung hat ebenso wie die weiteren evaluierten heimlichen polizeilichen Datenerhebungsmaßnahmen durch einen Richter zu erfolgen[602]; im Unterschied zu den übrigen Maßnahmen bleibt es hier allerdings bei der Zuständigkeit des Amtsgerichts.[603] Auch wenn nicht ersichtlich ist, warum hier abweichend von den übrigen Vorschriften an der ursprünglichen Zuständigkeit der Amtsgerichte festgehalten wird,[604] ist diese Regelung unter rechtlichen Aspekten nicht zu beanstanden.[605]

Auch bezüglich der weiteren verfahrensbezogenen Regelungen bestehen unter rechtlichen Aspekten keine Bedenken. Insbesondere der durch den DAV geäußerten Kritik, eine nachträgliche richterliche Kontrolle der Maßnahme könne nicht stattfinden, da keine Verpflichtung existiere, die von der Raster-

---

601 Landesregierung, LT-Drs. 14/2287, S. 52. In diesem Sinne auch *Roos/ Lenz*, POG, § 38 Rn. 7.

602 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09, Rn. 207: „Auch in verfahrensrechtlicher Hinsicht ist die Regelung [= § 20j BKAG] verhältnismäßig ausgestaltet, insbesondere verlangt sie die Anordnung durch einen Richter."

603 Zur Zuständigkeit des OVG vgl. die Ausführungen unter Ziff. 3.3.1.2.

604 Die Argumentation des Landesgesetzgebers zur Etablierung der Zuständigkeit des OVG bei Maßnahmen nach §§ 29, 31, 31b - e, nämlich die Intensität der Eingriffe und die Notwendigkeit „profunde[r] Kenntnisse des Verfassungs- und Verwaltungsrechts sowie entsprechende[r] Erfahrungen" (Landesregierung, LT-Drs. 15/4879, S. 30) ist auf den Bereich der Rasterfahndung übertragbar. Einziger Unterschied ist, dass hier ausschließlich ein Eingriff in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG im Raum steht, während bei den übrigen Maßnahmen auch die Art. 10 und 13 GG betroffen sind. Angesichts der Aussagen im Rasterfahndungsurteil des BVerfG (Urt. v. 04.04.2006 – 1 BvR 518/02) zur Grundrechtsintensität dieser Maßnahme, scheint eine solche Argumentation aber nicht zu greifen.

605 Vgl. hierzu die Ausführungen unter Ziff. 3.3.1.2.

fahndung Betroffenen zumindest im Nachhinein von der Maßnahme zu informieren,[606] greift nicht. Denn obwohl § 38 POG seinem Titel nach nur „Besondere Formen des Datenabgleichs“ regelt, stellt die Datenübermittlung, die die Polizei verlangen kann, gleichzeitig eine (heimliche) Datenerhebung durch die Polizei dar,[607] so dass hier die Regelungen des § 40 Abs. 5 und 6 POG eingreifen. Dabei dürfte sich wegen § 40 Abs. 6 S. 2 POG die Mitteilungspflicht auf die Personen beschränken, gegen die nach Abschluss der Rasterfahndung weitere Maßnahmen durchgeführt werden.[608]

3.3.9.5 Sicherung der Zweckbindung

§ 38 POG erlaubt grundsätzlich die Durchbrechung der Zweckbindung, da ursprünglich zu anderen Zwecken erhobene Daten nunmehr auch für die Gefahrenabwehr verwendet werden dürfen.[609] § 38 POG erlaubt nicht „nur“ eine nachträglich zweckändernde Verwertung von Zufallsfunden, wie dies beispielsweise § 29 Abs. 5 POG unter bestimmten Umständen tut. Vielmehr sollen bei der Rasterfahndung die Erkenntnisse „von vornherein gerade zu dem Zweck zusammengeführt und ausgewertet werden, einen Kreis von potentiellen Verdächtigen zu bestimmen, gegen den dann weitere personenbezogene Ermittlungsmaßnahmen gerichtet werden können. Übermittlung, Zusammenführung und Abgleich solcher Daten stellen eigenständige Eingriffe dar, die – anders als im Falle der strategischen Überwachung – von vornherein zu personenbezogenen Ermittlungszwecken erfolgen.“[610] Um sicherzustellen, dass

---

606 *Sandkuhl*, Stellungnahme DAV 69/2010, S. 9. *Schenke*, DVBl. 1996, 1393, 1400 hält es unter verfassungsrechtlichen Aspekten für hinnehmbar, wenn grundsätzlich keine Benachrichtigungspflicht von einer durchgeführten Rasterfahndung normiert wird; a.A. *Lisken*, NVwZ 2002, 513, 517, der von einer „gebotenen Benachrichtigung“ spricht.

607 Nach § 3 Abs. 2 Nr. 1 LDSG liegt eine Datenerhebung immer vor, wenn personenbezogene Daten beschafft werden.

608 So z.B. ausdrücklich Art. 44 Abs. 5 BayPAG. Da die Begründung zur bayerischen Einschränkung auf die Rechtslage in Rheinland-Pfalz übertragbar ist, vgl. *Käß*, BayVBl. 2009, 360, 365.

609 *Petri*, in: Lisken/ Denninger, Handbuch, Kapitel G, Rn. 531; *Horn*, DÖV 2003, 746, 748; *Roos/ Lenz*, POG, § 38 Rn. 4; *Robrecht*, SächsVBl. 2007, 80, 85. Grundsätzlich zur Zweckbindung BverfGE 65, 1, 46; vgl. auch *Tetsch*, in: Tetsch/ Baldarelli, PolG NRW, § 31 Ziff. 1.

610 BVerfG, Beschl. v. 04.04.2006 – 1 BvR 518/02, Rn. 132.

die mit der durch die Rasterfahndung veranlasste Aufhebung des Zweckbindungsgebots verbundenen weitreichenden Eingriffe in das Recht auf informationelle Selbstbestimmung nicht uferlos werden, sind die durch die Rasterfahndung selbst erlangten Daten einer strengen Zweckbindung zu unterwerfen; dem tragen sowohl § 38 Abs. 2 S. 2 und 3 sowie Abs. 4 S. 1 POG Rechnung: Zunächst dürfen „überschießend übermittelte“ Daten, mithin Daten, die nicht vom eigentlichen Ersuchen umfasst sind, deren Übermittlung aber aus (verfahrens-)ökonomischen Gründen dennoch erfolgt ist, nicht verwertet werden. Zudem sind nach Abschluss der Maßnahme sowohl sämtliche übermittelten als auch sämtliche durch den Abgleich generierten Daten zu löschen, „soweit sie nicht zur Verfolgung von Straftaten oder zur vorbeugenden Bekämpfung besonders schwerer Straftaten (§ 29 Abs. 2) erforderlich sind“, § 38 Abs. 4 S. 1 POG. Wegen der Ähnlichkeit von § 38 Abs. 4 S. 1 POG zur Regelung des vom BVerfG für verfassungswidrig erklärten § 20v Abs. 6 S. 5 BKAG[611] wäre eine Änderung des § 38 Abs. 4 S. 1 POG überlegenswert. Das BVerfG hat die Ausnahmeregelung des § 20v Abs. 6 S. 5 BKAG als verfassungswidrig eingestuft. Diese Vorschrift sieht ein Absehen von der Löschung auch nach Zweckerfüllung vor, soweit die Daten zur Verfolgung von Straftaten oder – nach Maßgabe des § 8 BKAG – zur Verhütung oder zur Vorsorge für die künftige Verfolgung einer Straftat mit erheblicher Bedeutung erforderlich sind. Sie erlaubt nach Auffassung des BVerfG damit die Speicherung der Daten in Blick auf eine Nutzung zu neuen, nur allgemein umschriebenen Zwecken, für die das Gesetz keine Ermächtigungsgrundlage enthalte und in dieser Offenheit auch nicht schaffen könne.[612]. Entsprechend der Kritik des BVerfG an der Kürze der Frist des § 20j Abs. 3 S. 3 BKAG[613], welche der Frist des § 38 Abs. 4 S. 3 POG entspricht, könnte letztere verlängert werden (→ Kapitel 3.3.10.1, S. 122 ff.).

3.3.10 Schutz des Kernbereichs privater Lebensgestaltung (§ 39a POG)

Entscheidungen zum Schutz des Kernbereichs privater Lebensgestaltung ergingen in dem Bereich der Strafverfolgung, des Verfassungsschutzes und des Polizeirechts.[614] Die Ausführungen der Gerichte für die Strafverfolgung

611 BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09, Rn. 274.

612 BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09, Rn. 274

613 BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09, Rn. 273, 272.

614 Vgl. nur BVerfG NJW 1973, 891; BVerfG NJW 2005, 2603, 2607; BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09.

und den Verfassungsschutz können auch für die polizeilichen Gefahrenabwehrregelungen fruchtbar gemacht werden.[615] Die entsprechende Vorschrift des § 160a StPO, die zwischen bestimmten Berufsgruppen differenziert, hat das BVerfG für verfassungskonform erachtet.[616]

3.3.10.1 Erhebungs- und Verwertungsverbot, Löschungs- und Dokumentationspflicht (§ 39a Abs. 1 POG)

Ob eine Information dem Kernbereich zuzuordnen ist, hängt davon ab, in welcher Art und Intensität sie aus sich heraus die Sphäre anderer oder Belange der Gemeinschaft berührt. Maßgebend sind die Besonderheiten des jeweiligen Einzelfalls. Zum Kernbereich gehören etwa Äußerungen innerster Gefühle oder Ausdrucksformen der Sexualität.[617] Der Schutz beschränkt sich nicht auf den räumlichen Bereich der Wohnung. Der Kernbereich kann auch bei Selbstgesprächen in einem Kraftfahrzeug berührt sein. Voraussetzung hierfür ist, dass die Nichtöffentlichkeit der Gesprächssituation bei einer Gesamtbewertung der Umstände des Einzelfalls derjenigen in einer Wohnung gleichzusetzen ist. Kriterien hierfür sind, ob das Risiko einer Außenwirkung der spontanen Äußerungen nahezu ausgeschlossen ist und das Selbstgespräch nur durch eine heimliche staatliche Überwachungsmaßnahme erfasst werden kann.[618]

Der verfassungsrechtlich gebotene Kernbereichsschutz lässt sich im Rahmen eines zweistufigen Schutzkonzepts gewährleisten: Auf der ersten Stufe durch ein Erhebungsverbot, auf der zweiten Stufe durch ein Verwertungsverbot. Das BVerfG führt dazu aus:[619]

> *„Die gesetzliche Regelung hat darauf hinzuwirken, dass die Erhebung kernbereichsrelevanter Daten soweit wie informationstechnisch und ermittlungs-technisch möglich unterbleibt. Insbesondere sind verfügbare informationstechnische Sicherungen einzusetzen. Gibt es im Einzelfall konkrete Anhaltspunkte dafür, dass eine bestimmte Datenerhebung den Kernbereich privater Lebensgestaltung berühren wird, so hat sie grundsätzlich zu unterbleiben. Anders liegt*

615 Vgl. BVerfG NJW 2008, 822, 832; BVerfG NJW 2004, 999, 1002; *Petri*, in Lisken/Denninger, Handbuch, Kapitel G, Rn. 29; a.A. noch *Haas* NJW 2004, 3082, 3084.

616 Vgl. BVerfG NJW 2012, 833, 840.

617 Vgl. BVerfG NJW 2012, 907, 908.

618 Vgl. BGH NJW 2012, 945, 946.

619 Vgl. BVerfG NJW 2008, 822, 834.

> *es, wenn zum Beispiel konkrete Anhaltspunkte dafür bestehen, dass kernbereichsbezogene Kommunikationsinhalte mit Inhalten verknüpft werden, die dem Ermittlungsziel unterfallen, um eine Überwachung zu verhindern. Entscheidende Bedeutung für den Schutz hat insoweit die Durchsicht der erhobenen Daten auf kernbereichsrelevante Inhalte, für die ein geeignetes Verfahren vorzusehen ist, das den Belangen des Betroffenen hinreichend Rechnung trägt. Ergibt die Durchsicht, dass kernbereichsrelevante Daten erhoben wurden, sind diese unverzüglich zu löschen. Eine Weitergabe oder Verwertung ist auszuschließen."*

Kritisiert wird an diesem Konzept etwa, dass es den Kernbereichsschutz in tatsächlicher Hinsicht abschwächt.[620] Für die zweite Stufe hält das BVerfG die Kontrolle durch eine unabhängige Stelle neben den Ermittlungsbehörden nicht mehr in allen Fallkonstellationen für zwingend erforderlich.[621] Denn der verfassungsrechtliche Bedarf für eine Sichtung durch eine unabhängige Stelle, d.h. für die dort vorgenommene Ausfilterung von Zweifelsfällen und Gewährleistung einer unabhängigen Kontrolle der dem Kernbereichsschutz dienenden Anforderungen[622], ist abhängig von der Schutzbedürftigkeit des Kernbereichs. Diese Schutzbedürftigkeit wird u.a. davon beeinflusst, welche Sozialbereiche erfasst werden, was an höchstprivaten Informationen erfasst wird sowie von den Schutzvorkehrungen auf der vorgelagerten Erfassungsebene[623]. Je geringer die Kernbereichsrelevanz einer Überwachung ist und je besser eine Erhebung der Daten kontrolliert und begrenzt werden kann, desto weniger Bedarf besteht für eine Kontrolle durch eine neutrale Stelle.

Zwei Konstellationen lassen sich in der Rechtsprechung des BVerfG hinsichtlich der Entbehrlichkeit einer unabhängigen Kontrolle der erhobenen Daten auf der Auswertungsebene erkennen. In einer dieser Konstellationen lässt das BVerfG (zumindest im Rahmen der Telekommunikationsüberwachung gemäß § 20l BKAG) eine Kontrolle auf der Erhebungsebene ausreichen und verneint die Notwendigkeit einer neutralen Sichtung auf der Aus- und Verwer-

---

620 Vgl. *Petri*, in Lisken/ Denninger, Handbuch, Kapitel G, Rn. 28.

621 Vgl. BVerfG NJW 2012, 833, 838, Rn. 222; BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09, Rn. 129.

622 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09, Rn. 204 zu § 20h BKAG (Wohnraumüberwachung).

623 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09, Rn. 204 zu § 20h BKAG (Wohnraumüberwachung)

tungsebene, und zwar insoweit, wie ein Erhebungsverbot auch für Zweifelsfälle die Erfassung wenigstens weitestgehend ausschließt.[624] Soweit Zweifelsfälle (im Falle des § 20l Abs. 5 S. 3 BKAG mittels automatischer Aufzeichnung) erfasst werden, bedarf es dann jedoch einer unabhängigen Sichtung etwa durch das die Überwachungsmaßnahme anordnende Gericht (wie im Falle des § 20l Abs. 5 S. 4 BKAG).[625] In einer weiteren Konstellation, in welcher für eine Überwachung der Telekommunikation gemäß § 100a StPO eine richterlichen Anordnung oder eine Bestätigung (§ 100b Abs. 1 S. 1 und 2 StPO) sowie eine Unterrichtung des anordnenden Gerichts über die Ergebnisse (§ 100b Abs. 4 S. 2 StPO) vorgeschrieben ist, verneint das BVerfG für die Datenerhebung die Notwendigkeit einer Beurteilung der gewonnenen Daten durch eine unabhängige Stelle.[626]

Ob das BVerfG eine gesetzliche Regelung zur Sicherstellung von Verwertungsverboten und Löschungsgeboten genügen lässt, hängt aber nicht nur von dem „Ob“ einer Kontrolle ab, sondern auch vom „Wie“. Was die Zusammensetzung der unabhängigen Stelle anbetrifft, so schließt das BVerfG jedenfalls für die Online-Überwachung die Mitwirkung (maximal) *eines*[627] durch gesonderte Verschwiegenheitspflichten abgesicherten Bediensteten des BKA zwecks Gewährleistung ermittlungsspezifischen Sachverstandes nicht aus,[628] verlangt aber, dass die tatsächliche Durchführung und Entscheidungsverantwortung maßgeblich in den Händen dem BKA gegenüber unabhängiger Personen liegen.[629] Für den Zeitpunkt der Kontrolle stellt sich das BVerfG eine frühzeitige Beteiligung der neutralen Stelle vor, so dass kernbereichsrelevante Daten möglichst vor Kenntnisnahme der Sicherheitsbehörde ausgefiltert werden[630]. Nach Ansicht des BVerfG kann (zumindest) für die Wohnraumüberwachung

---

624 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09, Rn. 241.

625 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09, Rn. 245.

626 BVerfG, NJW 2012, 833, 838, Rn. 223, 224.

627 Kursiv hervorgehoben in BVerfG, Urt. v. 20.04.2016 –1 BvR 966/09 und 1 BVR 1140/09, Sondervotum Schuckebier, Rn. 14.

628 BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BVR 1140/09, Rn. 224 zu § 20k BKAG (Online-Durchsuchung).

629 BVerfG, Urt. v. 20.04.2016 –1 BvR 966/09 und 1 BVR 1140/09, Rn. 224 zu § 20k BKAG (Online-Durchsuchung).

630 Vgl. BVerfG, Urt. v. 20.04.2016 –1 BvR 966/09 und 1 BVR 1140/09, Rn. 129 und 224 zu § 20k BKAG (Online-Durchsuchung).

der Gesetzgeber besondere Regelungen für – in der Praxis eher häufiger vorkommenden[631] – Ausnahmefälle bei Gefahr im Verzug treffen.[632]

Mit dem Ziel, den Anforderungen des BVerfG an den Schutz des Kernbereichs zu entsprechen, sieht § 39a POG ein Zusammenspiel von Erfassungs- und Verwertungsebene vor, das wie folgt in drei verschiedene Gruppe eingeteilt werden könnte. Die *erste Gruppe* sind – unabhängig von der Überwachungsmaßnahme – auf Erfassungsebene erkannte Eingriffe in den Kernbereich privater Lebensgestaltung, welche damit auf der Erfassungsebene bereits die Erhebung verhindern[633]. Die *zweite Gruppe* sind – bei Erhebungen nach §§ 29, 31, 31c POG – auf der Erfassungsebene als Zweifelsfälle eingestufte Situationen, welche auf der Verwertungsebene einer gerichtlichen Entscheidung über die Verwertung unterliegen[634]. Die *letzte Gruppe* sind diejenigen Konstellationen, welche auf Erfassungsebene – im Falle von Erhebungen nach § 31b POG – als Zweifelsfälle betrachtet werden[635] bzw. – unabhängig von der Art der Überwachungsmaßnahme – die Fälle, bei denen eine Betroffenheit des Kernbereichs nicht gesehen wird. Diese unterliegen auf Verwertungsebene einer Durchsicht durch die Polizei selber, über welche das Gericht eine Sachleitung hat.[636]

Zu den übergreifenden Verhältnismäßigkeitsanforderungen gehört auch die Regelung von Löschungspflichten[637]. Schriftlich zu dokumentieren ist bei einer Löschung nur, dass es zur Aufnahme absolut geschützter Gesprächsinhalte gekommen ist und dass die diesbezüglichen Aufzeichnungen deswegen vollständig gelöscht worden sind. Jede darüber hinausgehende aussagekräftige Dokumentation würde gegen das absolute Verbot der Erhebung kernbereichsrelevanter Informationen verstoßen. Unbefriedigt bleibt danach zwar ein mögliches Interesse des Betroffenen an vollständiger Kenntnis darüber,

---

631 BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BVR 1140/09, Sondervotum *Schluckebier*, Rn. 16.

632 BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BVR 1140/09, Rn. 129 und 204 zu § 20h BKAG (Wohnraumüberwachung).

633 Vgl. § 39a Abs. 2, 3, 5 S. 1 POG. Vgl. zu § 39a Abs. 5 S. 1 POG die LT-Drs. 15/4879, S. 44: „In Satz 1 wird der allgemeine Begriff „unmittelbare Kenntnisnahme einer Maßnahme nach den §§ 29, 31 und 31c“ anstelle der bisherigen Aufzählung „Abhören, die Beobachtung sowie die Auswertung der erhobenen Daten“ verwendet.“.

634 Vgl. § 39a Abs. 5 S. 1, 2 POG.

635 Arg. e contr. aus § 39a Abs. 5 S. 1, 2 POG.

636 Vgl. § 39a Abs. 4 POG.

637 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09, 1 BVR 1140/09, Rn. 144.

welche Gesprächsinhalte überwacht worden sind[638]. Dies ist jedoch notwendige Konsequenz des Kernbereichsschutzes im Bereich der Wohnraumüberwachung, dem gerade auch das Absehen von einer automatischen Aufzeichnung dient.[639] Eine Frist zur Löschung der Löschungsprotokolle, wie sie vom BVerfG in den Fällen der Wohnraumüberwachung gemäß § 20h Abs. 5 S. 10 BKAG[640], der Online-Durchsuchung gemäß § 20k Abs. 7 S. 8 BKAG[641], der Telekommunikationsüberwachung gemäß § 20l Abs. 6 S. 10 BKAG[642], der Rasterfahndung gemäß § 20j Abs. 3 S. 3 BKAG[643] und allgemein gemäß § 20v Abs. 6 S. 3 BKAG[644] wegen ihrer Kürze kritisiert wurde, findet sich im POG nicht.

3.3.10.2 Voraussetzung für eine Anordnung nach § 29 POG (§ 39a Abs. 2)

Die Bestimmung ist an die Formulierung in § 100c Abs. 4 StPO angelehnt. Die Regelung in § 100c Abs. 4 StPO hat das BVerfG für verfassungsgemäß erachtet.[645] Nur die letzten beiden Sätze in § 100c Abs. 4 StPO, die den Kernbereich näher abgrenzen, wurden nicht ins POG übernommen. Allerdings ist der Gesetzgeber von Verfassung wegen nicht verpflichtet, den Kernbereich positiv, unter Nennung der in dem Urteil des BVerfG angeführten Beispiele gesetzlich zu definieren. Zwar besteht eine Vermutung für den Kernbereich bei Räumen, denen typischerweise oder im Einzelfall die Funktion als Rückzugsbereich der privaten Lebensgestaltung zukommt. Eine Vermutungsregel in das Gesetz aufzunehmen ist allerdings nicht erforderlich.[646] Die Ausgestaltung im Einzelnen ist Aufgabe des zuständigen Gesetzgebers, dem hierbei ein weiter Beurteilungs- und Gestaltungsspielraum zukommt. Im Rahmen dieses Gestaltungsspielraums darf sich der Gesetzgeber auch unbestimmter, auslegungsbedürftiger Rechtsbegriffe bedienen. Das Grundgesetz fordert nicht, dass der Schutz

638 Vgl. BVerfG NJW 2012, 907, 908, Rn. 104; BVerfG, NJW 2004, 999, 1007.

639 Vgl. BVerfG NJW 2012, 907, 908, Rn. 104.

640 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09, 1 BVR 1140/09, Rn. 205.

641 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09, 1 BVR 1140/09, Rn. 226.

642 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09, 1 BVR 1140/09, Rn. 246.

643 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09, 1 BVR 1140/09, Rn. 272.

644 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09, 1 BVR 1140/09, Rn. 273.

645 Vgl. BVerfG NJW 2007, 2753, 2755.

646 Vgl. BVerfG NJW 2007, 2753, 2755.

des unantastbaren Bereichs privater Lebensgestaltung durch umfangreiche, detailfreudige Regelungen geregelt wird[647] .

Was die Verfassungsmäßigkeit des Schutzes des Kernbereichs auf den Stufen der Erfassung und Verwertung der Daten aus der Wohnraumüberwachung nach § 29 POG betrifft, so spricht deren tief in die Privatsphäre eindringender Eingriff vom Grundsatz her für die Erforderlichkeit einer unabhängigen Kontrolle auf der Verwertungsebene, welche umfassend für alle nicht bereits auf der Erfassungsebene ausgeschiedenen Daten den Schutz des Kernbereichs sicherstellt, d. h. sowohl für solche Daten, bei denen Anlass bestand, eine Kernbereichsrelevanz zu vermuten, wie auch für Daten, bei denen kein solcher Anlass bestand. Das BVerfG verlangt auf Verwertungsebene eine unabhängige Sichtung, welche sowohl Zweifelsfälle herausfiltert wie auch insgesamt eine unabhängige Kontrolle der dem Kernbereichsschutz dienenden Anforderungen gewährleistet[648].

Eine ausreichende Kontrolle sieht das BVerfG als gegeben, wenn wie im Fall des § 20h Abs. 5 S. 4 BKAG die Daten von der Erfassungsebene direkt an ein Gericht zur Entscheidung über Verwertbarkeit oder Löschung der Daten gegeben werden[649], was dort allerdings nur bei den automatisch aufgezeichneten Zweifelfällen erfolgt[650]. Damit dürfte auch bei automatischen Aufzeichnungen, bei denen Anlasspunkte für eine Kernbereichsrelevanz bestehen, mit der Sichtung durch ein Gericht gemäß § 39a Abs. 5 S. 2 POG eine ausreichende unabhängige Kontrolle vorliegen.

Für nicht akzeptabel erachtet das BVerfG hingegen, dass diese unabhängige Sichtung im BKAG auf automatischen Aufzeichnungen in Zweifelsfällen (§ 20h Abs. 5 S. 4 BKAG) beschränkt ist[651] (und mithin Daten, bei denen keine Kernbereichsrelevanz vermutet wurde, nicht erfasst). Hier hat der Gesetzgeber sich ersichtlich von der Erwägung leiten lassen, dass eine weitere unabhängige Sichtung nicht erforderlich ist, weil die Erfassung von höchstpersönlichen Informationen bei richtiger Gesetzesanwendung auf der Erhebungsstufe durch § 20h Abs. 5 S. 1 und 2 BKAG ausgeschlossen werde. [652] In Anbetracht der Ziele solcher Sichtungen (u.a. Herausfiltern von Zweifelsfällen und

---

647 Vgl. BVerfG NJW 2007, 2753, 2755.

648 BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09, Rn. 204

649 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BVR 1140/09, Rn. 204.

650 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BVR 1140/09, Rn. 204.

651 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BVR 1140/09, Rn. 204.

652 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BVR 1140/09, Rn. 204.

Gewährleistung einer unabhängigen Kontrolle der dem Kernbereichsschutz dienenden Anforderungen insgesamt) lässt sich eine solche Beschränkung der unabhängigen Sichtung allerdings nicht rechtfertigen. [653].

Die Gestaltung der angeordneten Kontrollregelungen des POG auf Verwertungsebene scheint hierfür gleichfalls nicht zu genügen. Zwar hat der rheinland-pfälzische Gesetzgeber hier Regelungsbedarf gesehen und statuiert in § 39a Abs. 4 POG eine Überwachung, innerhalb derer dem anordnenden Gericht eine Sachleitung (→ Kapitel 3.3.10.4, S. 133 ff.) an die Hand gegeben wird, mit welcher es zu Vorgaben und Prüfung von deren Umsetzung ermächtigt ist, sowie eine Kontrolle durch zwei Polizeibeamte und einen Datenschutzbeauftragten (→ Kapitel 3.3.10.4.4, S. 141 f.) und zudem in § 29 Abs. 4 POG eine fortlaufende Unterrichtung des Gerichts. Des Weiteren sind auch im Falle von bei der Auswertung[654] wahrgenommenen Anhaltspunkten für eine Kernbereichsrelevanz die Daten dem OVG zur Entscheidung über die Verwertbarkeit gemäß § 39a Abs. 5 S. 2 POG vorzulegen. Die Sachleitung des Gerichts aus § 39a Abs. 3 POG (welche anders als etwa in § 20k Abs. 7 S. 3 BKAG näher ausgeformt ist) und die fortlaufende Unterrichtung aus § 29 Abs. 4 POG mögen zwar eine unabhängige, wenngleich nur mittelbare, Kontrolle leisten, bieten aber nicht einen der polizeilichen Verwertung bzw. Kenntnisnahme vorgeschalteten Filter. Dies gilt auch für die Unterbrechung einer schon im Bereich der Polizei begonnenen Kenntnisnahme von Daten, und deren Weiterleitung an das OVG zwecks Kontrolle gemäß § 39a Abs. 5 S. 1 und 2 POG.

Aus einem Urteil des BVerfG zu auf Altfassungen des § 29 POG gestützten Lauschangriffen kann für die Auffassung des BVerfG zur Norm des POG nichts gewonnen werden, da die Verfassungsbeschwerden eine Verletzung des Kernbereichs privater Lebensgestaltung nicht hinreichend substantiiert dargelegt haben[655]. Im Ergebnis scheint daher die Norm in ihrer jetzigen Fassung den Vorstellungen des BVerfG zu Notwendigkeit und Ausgestaltung einer unabhängigen Kontrolle auf Verwertungsebene allein für Zweifelsfälle zu genügen und bedürfte für Nicht-Zweifelsfälle noch einer unabhängigen, vorherigen Kontrolle mit maximal einem Polizeibediensteten.

---

653 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BVR 1140/09, Rn. 204.

654 Vgl. LT-Drs. 15/48789, S. 44: „In Satz 1 wird der allgemeine Begriff »unmittelbare Kenntnisnahme« einer Maßnahme nach den §§ 29, 31 und 31c POG anstelle der bisherigen Aufzählung »Abhören, die Beobachtung sowie die Auswertung der erhobenen Daten« verwendet“.

655 BVerfG, NJW 2012, 907, 908, Rn. 95.

3.3.10.3 Voraussetzung für eine Anordnung nach §§ 31, 31b, 31c POG (§ 39a Abs. 3)

Während nach § 39a Abs. 2 POG eine Datenerhebung bei einer Wohnraumüberwachung angeordnet werden darf, *soweit nicht* der Kernbereich privater Lebensgestaltung betroffen ist, können nach § 39a Abs. 3 POG die TKÜ und die Online-Durchsuchung angeordnet werden, falls nicht davon auszugehen ist, dass *allein* Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden. Der Kernbereichsschutz ist für die letztgenannten Maßnahmen somit geringer als für die Wohnraumüberwachung.[656] Im praktischen Leben sei es wohl sehr selten, dass allein kernbereichsrelevante Inhalte kommuniziert werden.[657] Der Kernbereichsschutz der ersten Stufe laufe so ins Leere.[658] Die herrschende Ansicht hält diese Formulierung für verfassungswidrig.[659] Es sei kein Fall denkbar, in dem auf einem Computer allein kernbereichsrelevante Daten gespeichert sind.[660] In den Gesetzesbegründungen wird dage-

---

656 In Bayern heißt es dagegen in Art. 34d Abs. 1 S. 5, 6 BayPAG: „Soweit dies informationstechnisch und ermittlungstechnisch möglich ist, hat die Polizei durch geeignete Vorkehrungen sicherzustellen, dass die Erhebung von Daten unterbleibt, die dem Kernbereich der privaten Lebensgestaltung zuzurechnen sind. Wird erkennbar, dass solche Daten betroffen sind und bestehen keine Anhaltspunkte dafür, dass diese Daten dem Zweck der Herbeiführung eines Erhebungsverbots dienen sollen, ist die Maßnahme insoweit unzulässig."

657 Vgl. *Hoffmann-Riem*, JZ 2008, 1009, 1021; *Kugelmann*, BKA-Gesetz, § 20k, Rn. 18; § 20l, Rn. 16

658 Vgl. *Poscher*, JZ 2009, 269, 276; *Sandkuhl*, Stellungnahme DAV, S. 15; *Kugelmann*, BKA-Gesetz, § 20k Rn. 18: „kaum geeignet, den Grundrechtsschutz effektiv zu sichern", § 20l, Rn. 16: „Quasi-Ausschluss des Kernbereichschutzes".

659 Vgl. *Albrecht/ Dienst*, JurPC 5/2012, Abs. 11; *Ritter*, Vorratsdatenspeicherung, S. 229 zu § 100a Abs. 4 StPO; *Hoffmann*, Vertraulichkeit, S. 116 zu § 20k BKAG; *Bäcker*, BKA, S. 89 m.w.N. zu § 20k BKAG; *Bäcker*, IT-Grundrecht, S. 28 f zu § 20k BKAG; *Gudermann*, Onlinedurchsuchung, S. 253 zu § 20 BKAG; *Puschke/ Singelnstein*, NJW 2008, 113, 114 zu § 100a StPO; *Globig*, 41. Sitzung des Innenausschusses vom 04.11.2010, Teil II, S. 16; *Breyer*, 41. Sitzung des Innenausschusses am 04.11.2010, Teil II, S. 36; *Roggan*, NJW 2009, 257, 261 zu § 20k BKAG; *Baum/ Schantz*, ZRP 2008, 137, 138 zu § 20k BKAG; unproblematisch bei *Rühle*, POG, Kap. G, Rn. 77; a.A. *Bär*, MMR 2008, 215, 217.

660 Vgl. *Kutscha*, DuD 2012, 391, 393; Zabel, JR 2009, 453, 457 zu § 20k BKAG.

gen auf den Fall verwiesen, dass der Betroffene kernbereichsrelevante mit gefahrenrelevanten Inhalten verknüpft, um die Maßnahme zu verhindern.[661]

Entgegen den erwähnten Bedenken ist die Vorschrift mit dem Verfassungsrecht vereinbar. Das BVerfG hat die entsprechend formulierte Regelung der Telekommunikationsüberwachung in § 100a Abs. 4 StPO[662] und in § 20l Abs. Abs. 6 S. 1 BKAG[663] sowie der Online-Durchsuchung § 20k Abs. 7 S. 1 BKAG[664] in aktuellen Entscheidungen nicht beanstandet. Das BVerfG präzisiert darin seine zum kernbereichsrechtlichen Schutzkonzept aufgestellten Grundsätze. In § 100a Abs. 4 S. 1 (und in ähnlicher Form in § 20k Abs. 7 S. 1 BKAG; § 20l Abs. 6 S. 1 BKAG) heißt es:

> *„Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch eine Maßnahme nach Absatz 1 allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, ist die Maßnahme unzulässig.“*

Die Formulierung stellt sicher, dass eine zielgerichtete Erhebung kernbereichsrelevanter Daten unterbleibt. Die praktischen Schwierigkeiten sowohl bei einer automatischen als auch bei einer persönlichen Überwachung gebieten es, den Kernbereichsschutz auf die zweite Stufe zu verlagern. Dies gilt sogar dann, wenn es sich um eine persönliche Überwachung von Personen handelt, die sich in klarem Deutsch miteinander unterhalten.[665]

Die Verfassungswidrigkeit ergibt sich auch nicht aus einem Vergleich zu § 39a Abs. 2 POG, wonach bei der Wohnraumüberwachung die Datenerhebung nur angeordnet werden darf, soweit nicht aufgrund tatsächlicher Anhaltspunkte anzunehmen ist, dass durch die Überwachung Daten erhoben werden, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind.

---

661 Vgl. Landesregierung, LT-Drs. 15/4879, S. 44 zu § 39a Abs. 3 POG; CDU/CSU und FDP, BT-Drs. 16/9588, S. 77 zu § 20k BKAG.

662 Vgl. BVerfG NJW 2012, 833, 837-838, Rn. 209-224; das BVerfG (BVerfG NJW 2013, 833, 837) erklärt ausdrücklich, dass seine Überlegungen für die Onlinedurchsuchung entsprechend gelten; ebenso ThürVerfGH, Urt. v. 21.11.2012 – VerfGH 19/09 zu § 34b Abs. 1 ThürPAG.

663 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09, Rn. 243.

664 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09, Rn. 222.

665 Vgl. BVerfG NJW 2012, 833, 837 f; kritisch dazu *Roggan*, HRRS 2013, 153, 157 und 158, der im Übrigen die Meinung vertritt, eine Echtzeitüberwachung könne aus Verhältnismäßigkeitsgründen vorzuziehen sein.

Für die rechtliche Unterscheidung spricht, dass bei der Überwachung der Telekommunikation der Schutz weniger stark ausgestaltet werden muss. Die Bürger sind zur höchstpersönlichen Kommunikation auf den Fernmeldeverkehr nicht in gleicher Weise angewiesen wie auf eine Wohnung[666], für die der Rückzugsbereich der privaten Wohnung die höchstvertrauliche Kommunikation nach Verständnis des BVerfG gerade typusprägend ist[667]. Entsprechendes wie für den Fernmeldeverkehr müsste auch für die Online-Durchsuchung und die Auskunft über Nutzungsdaten gelten.[668]

Bei der Überwachung der Telekommunikation gemäß § 31 POG stellt sich die Situation hinsichtlich des Schutzes des Kernbereichs auf den Stufen der Erhebung und der Auswertung anders dar als im Rahmen des § 29 POG. Für Telekommunikationsüberwachungen bestehen geringere Anforderungen an den Kernbereichsschutz[669], da für sie ein höchstvertraulicher Austausch nicht typusprägend ist[670] und sie weniger tief als Wohnraumüberwachung und Online-Durchsuchung in die Privatsphäre eindringen[671]. Angesichts der geringeren Grundrechtsrelevanz hat hier das BVerfG die in § 20l Abs. 6 POG ähnlich zu § 39a Abs. 5 POG ausgestaltete Wechselwirkung von Kontrolle auf Erfassungs- und Verwertungsebene getrennt nach automatisiert erfassten Zweifelsfällen und sonstigen Fällen für ausreichend erachtet. Es genügt also, dass allein Zweifelsfälle (oder in der Formulierung des § 39a Abs. 5 S. 1 POG und ähnlich in § 20l Abs. 6 BKAG: „sofern sich tatsächliche Anhaltspunkte ergeben, dass Inhalte, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, erhoben werden“) einer gerichtlichen Entscheidung über der Verwertbarkeit unterliegen, nicht aber die sonstigen Fälle[672].

Der Kernbereichsschutz aus § 39a POG ist für den Bereich der Telekommunikationsüberwachung sogar noch etwas stärker als im BKAG. Denn die Auswertung der Daten durch die Polizei erfolgt unter der Sachleitung des OVG

---

666 Vgl. BVerfG NJW 2005, 2603, 2612; ThürVerGH, Urt. v. 21.11.2012, 19/09.

667 Siehe BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09, Rn. 238.

668 Sollte sich der Gesetzgeber für eine Einbeziehung des § 31b POG in § 39a POG entscheiden, wären die obigen Ausführungen auch auf diese Norm übertragbar.

669 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BVR 1140/09, Rn. 239 (zur Telekommunikationsüberwachung nach § 20l BKAG).

670 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, Rn. 238.

671 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, Rn. 238.

672 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, Rn. 241.

gemäß § 39a Abs. 4 S. 1 POG. Zudem ist auch für den Fall, dass auf Verwertungsebene bei der Kenntnisnahme, was gemäß der Begründung des Gesetzesentwurfes auch die Auswertung umfasst[673], Zweifelsfälle erkennbar werden, eine gerichtliche Kontrolle vorgeschrieben.

Was den Kernbereichsschutz im Rahmen der Quellen-Telekommunikationsüberwachung betrifft, so unterscheidet das BVerfG wie das POG (oder das BKAG) nicht zwischen der Telekommunikationsüberwachung (§ 31 Abs. 1, 2 POG) und der Quellentelekommunikationsüberwachung (§ 31 Abs. 3 POG).

Der Kernbereichsschutz für die Online-Durchsuchung gemäß § 31c POG ist dagegen wieder ähnlich wie bei der Wohnraumüberwachung zu bewerten. Das BVerfG hat hier das in § 20k Abs. 7 BKAG normierte Schutzprogramm für nicht hinreichend erachtet. Anders als das POG unterscheidet § 20k Abs. 7 BKAG nur zwei Fallgruppen, auf Erhebungsebene erkannte und damit aus der Überwachung ausscheidende Kernbereichsdaten, was das BVerfG als verfassungskonform betrachtet[674], und sonstige Daten, welche auf Verwertungsebene gemäß § 20k Abs. 7 S. 3 BKAG von unter einer gerichtlichen Sachleitung (→ Kapitel 3.3.10.4, S. 133 ff.) stehenden Personen, zwei BKA-Bediensteten und dem – hier weisungsfreien – Datenschutzbeauftragten (→ Kapitel 3.3.10.4.4, S. 141 f.), durchzusehen sind. Den genannten Maßnahmen fehlt es an verfassungsrechtlich hinreichenden Vorkehrungen auf der Ebene des nachgelagerten Kernbereichsschutzes. § 20k Abs. 7 S. 3, 4 BKAG sieht keine hinreichend unabhängige Kontrolle vor.[675] Das BVerfG verlangt hier, dass – damit die tatsächliche Durchführung und Entscheidungsverantwortung maßgeblich in den Händen dem BKA gegenüber unabhängiger Personen liege – die Hinzuziehung (maximal) *eines*[676] durch gesonderte Verschwiegenheitspflichten abgesicherten Bediensteten des BKA möglich sei,[677], und dass die Beteiligung der neutralen Stelle so frühzeitig erfolge, dass kernbereichsrelevante Daten möglichst vor Kenntnisnahme der Sicherheitsbehörde ausgefiltert werden[678].

---

673 LT-Drs. 15/4879, S. 44.

674 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BVR 1140/09, Rn. 222.

675 BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BVR 1140/09, Rn. 223 (zu § 20k BKAG (Online-Durchsuchung).

676 Kursiv hervorgehoben in BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09, 1 BVR 1140/09, Sondervotum *Schluckebier*, Rn. 14.

677 BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BVR 1140/09, Rn. 224 (zu § 20k BKAG (Online-Durchsuchung).

678 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BVR 1140/09, Rn. 129 und 224 zu § 20k BKAG (Online-Durchsuchung)

Die im POG in drei unterschiedlichen Fallgruppen ablaufende Kontrolle entspricht diesen Forderungen des BVerfG nur in zwei Fallgruppen. Während die erste Fallgruppe der erkannten Kernbereichsfälle bereits unproblematisch[679] auf Verwertungsebene gemäß § 39a Abs. 1, 3, 5 POG ausscheidet und für die – im Rahmen des § 20k BKAG nicht enthaltene – Fallgruppe der automatisiert aufgezeichneten Zweifelfälle eine gerichtliche Kontrolle vorgesehen ist, welche entsprechend den Überlegungen des BVerfG zur von ihm gebilligten gerichtlichen Sichtung aus § 20h Abs. 5 S. 4 BKAG[680] nicht zu beanstanden ist, ist bei der dritten Gruppe der sonstigen erhobenen Daten, welche auf Verwertungsebene wie im Rahmen des § 39a Abs. 4 S. 2 POG durch zwei Polizeibeamte und den behördlichen Datenschutzbeamten unter gerichtlicher Sachleitung gesichtet wird, nach den Überlegungen des BVerfG der Kernbereich der privaten Lebensgestaltung nicht im ausreichendem Maße durch eine unabhängige Kontrolle geschützt.

3.3.10.4 POG Sachleitung des OVG (§ 39a Abs. 4)

Die Sachleitung des OVG führt zu rechtlichen Problemen, die im Folgenden behandelt werden. Dazu gehört die Normenbestimmtheit, die Frage, ob es sich um Rechtsprechungs-tätigkeit handelt und ob das Verfahren für den Kernbereichsschutz geeignet ist.

3.3.10.4.1 Normenbestimmtheit

Die Bestimmtheit der Vorschrift wurde von den Beschwerdeführern im Verfahren gegen das BKAG bezweifelt.[681] Es sei nicht erkennbar, was mit dem Begriff der Sachleitung gemeint ist. Das BVerfG hat sich dazu nicht weiter geäu-

679 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BVR 1140/09, Rn. 222 (zu § 20k BKAG).

680 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BVR 1140/09, Rn 204.

681 Vgl. Vorbringen der Beschwerdeführer in dem Urteil des BVerfG v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09, Rn. 30; vgl. auch die Formulierung des BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09, Rn. 225: „allgemeine bleibende Sachleitung des anordnenden Gerichts“. Ähnlich auch *Schenke*, in: Schenke/ Graulich/ Ruthig, Sicherheitsrecht des Bundes, § 20k Rn. 46, und *Roggan*, NJW 2009, 257, 261.

ßert, sondern nur festgestellt, dass es eine „allgemein bleibende „Sachleitung““ sei[682]. Auch im Gesetzgebungsverfahren wurde darüber diskutiert, welche Pflichten mit einer Sachleitung verbunden sind. Während der Gesetzesentwurf zur Änderung des BKAG über die Sachleitung nichts weiter ausführt,[683] heißt es in der Begründung zum Entwurf des POG: „Das Oberverwaltungsgericht Rheinland-Pfalz leitet die Auswertung der erhobenen Daten, prüft und trifft die erforderlichen Maßnahmen.“[684] Im Innenausschuss wurden Bedenken erhoben, dass das OVG zwar einbezogen werde, aber nicht von sich aus, sondern vielmehr erst auf Anfrage tätig werden dürfe.[685] Auf einen Antrag von SPD, CDU und FDP[686] wurde die Vorschrift um den jetzigen Satz 2 ergänzt, wonach es heißt: „Es [das OVG] gibt insbesondere die für die Prüfung einer Kernbereichsrelevanz erforderlichen Vorgaben und überprüft deren Realisierung.“ Daraus wird nun gefolgert, dass das Gericht Vorgaben machen und deren Realisierung überprüfen *muss*.[687]

Der Begriff der Sachleitung oder Sachleitungsbefugnis findet im Zusammenhang mit strafrechtlichen Vorschriften Erwähnung. So enthält der mit Verhandlungsleitung überschriebene § 238 StPO eine Sachleitungsbefugnis.[688] Dazu gehören alle Maßnahme der Durchführung der Hauptverhandlung, insbesondere Eröffnung, Durchführung, Unterbrechung und Schließung der Verhandlung und die Bestimmung des Verfahrensgangs.[689] In den Verfassungsschutzgesetzen wird auf die Sachleitungsbefugnis der Staatsanwaltschaft verwiesen.[690] In der Literatur findet sich der Begriff der Sachleitungsbefugnis der

682 Siehe BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09, Rn. 225.

683 Vgl. Bundesregierung, BT-Drs. 16/10121, S. 31; *Schenke*, in: Schenke/ Graulich/ Ruthig, Sicherheitsrecht des Bundes, § 20k BKAG Rn. 46.

684 Vgl. Landesregierung, LT-Drs. 15/4879, S. 44.

685 Vgl. *Globig* in der 41. Sitzung des Innenausschusses am 04.11.2010, Teil II, S. 16.

686 Vgl. Landesregierung, LT-Drs. 15/5332, S. 2.

687 Vgl. *Roos/ Lenz*, POG, § 39a Rn. 7.

688 Vgl. *Gorf*, in: Graf, StPO, § 238 Rn. 3 ff.

689 Vgl. *Meyer-Goßner*, in: Meyer-Goßner/ Schmitt, StPO, § 238 Rn. 5.

690 Vgl. nur § 14 Abs. 2 RPfLVerfSchG, § 10 BWLVSG, § 18 Abs. 1 BverfSchG.

Staatsanwaltschaft.[691] Verwendet wird auch die Bezeichnung Verfahrensleitung[692] oder Verfahrenshoheit[693] oder Leitungsbefugnis.[694] Dazu gehören die Rechtskontrolle und die Grundverantwortung für die richtige Beschaffung und Zuverlässigkeit des im Justizverfahren benötigten Beweismaterials.[695] Der BGH führt dazu aus:

> *„Auf Grund dieser umfassenden Verantwortung steht der StA gegenüber ihren Ermittlungspersonen ein uneingeschränktes Wiesungsrecht in Bezug auf ihre auf die Sachverhaltserforschung gerichtete strafverfolgende Tätigkeit zu. Dabei kann sie konkrete Einzelweisungen zu Art und Durchführung einzelner Ermittlungshandlungen erteilen, Nrn. 3 II, 11 RiStBV, oder ihre Leitungsbefugnis im Rahmen der Aufklärung von Straftaten unabhängig vom Einzelfall durch allgemeine Weisungen im Voraus in Anspruch nehmen.“*[696]

Überträgt man diese Grundsätze auf die gefahrenrechtliche Überprüfung des Kernbereichsschutzes, so bedeutet das:

- Das OVG hat die Verfahrensherrschaft über die Frage der Auswertung der Daten.
- Es ist befugt, das Verfahren der Auswertung zu eröffnen, durchzuführen, zu unterbrechen und für beendet zu erklären.
- Das OVG ist zuständig für die rechtliche Überprüfung des Kernbereichs und trägt die rechtliche Grundverantwortung. Es kann gegenüber den für die Auswertung zuständigen Polizeibeamten Weisungen erteilen, soweit es die Auswertung der Daten betrifft.
- Die Grundentscheidung trifft also das Gericht, nicht die polizeilich zur Durchsicht Befugten. Dadurch, dass die Realisierung gerichtlich überprüft

---

691 Vgl. *Moldenhauer*, in: KK-StPO, § 163d Rn. 32; *Patzak*, in: Graf, StPO, § 160 Rn. 6; *Hegmann*, in: Graf, StPO, § 110, Rn. 7; *Gercke/ Temming*, in: Gercke u.a., StPO, § 160, Rn. 81; *Zöller*, in: Gercke u.a., StPO,§ 167 Rn. 1.

692 Vgl. *Pfeiffer*, in: Pfeiffer, StPO, § 100d Rn. 1; *Diemer*, in: KK-StPO, § 155b Rn. 2; *Ahlbrecht*, in: Gercke u.a., StPO, § 131 Rn. 8.

693 Vgl. *Griesbaum*, in: KK-StPO, § 161 Rn. 27; *Zöller*, in: Gercke u.a., StPO, § 161, Rn. 26, § 163 Rn. 3, 5.

694 Vgl. *Griesbaum*, in: KK-StPO, § 161 Rn. 27; *Pfeiffer*, in: Pfeiffer, StPO, § 161 Rn. 8.

695 Vgl. *Schmitt*, in: Meyer-Goßner/ Schmitt, § 163 Rn. 3.

696 Vgl. BGH NJW 2009, 2612, 2613.

werden muss, kann ein Missbrauch der Behörden verhindert werden.[697] Das Gericht kann von der Polizei einen Bericht über die Einhaltung des Kernbereichs anfordern.[698]

- Daraus folgt, dass eine Überprüfung der Daten im Einzelfall durch das OVG grundsätzlich nicht erforderlich ist.[699] Eine Grundverantwortung ist mit der rechtlichen Prüfung der Daten durch das Gericht nicht gleichzusetzen. Dafür spricht auch die Verteilung der Zuständigkeiten zwischen der Polizei und dem Gericht. Eine Durchsicht durch die Polizei wäre sinnlos, wenn das Gericht als unabhängige Instanz dieselbe Kontrolle durchführen müsste.
- Das OVG muss von seiner Sachleitungsbefugnis Gebrauch machen. Dafür spricht die Gesetzesbegründung. Das polizeirechtliche Opportunitätsprinzip passt insoweit nicht. Das Auswahlermessen zielt in eine andere Richtung: Es ermöglicht den Einsatz verschiedener Mittel für die Gefahrenbekämpfung.[700] Die Sachleitungsbefugnis betrifft vorliegend die Auswertung der Daten. Zweck der Vorschrift ist der Schutz des Kernbereichs privater Lebensgestaltung und verwirklicht den Grundrechtsschutz durch Verfahren.

Der Begriff der Sachleitung ist durch Auslegung bestimmbar. Auch vor dem Hintergrund der hohen Anforderungen an die Normenklarheit und -bestimmtheit bei datenschutzrechtlichen Maßnahmen[701] genügt der Begriff den verfassungsrechtlichen Anforderungen. Insoweit handelt es sich um einen unbestimmten Rechtsbegriff ohne Beurteilungsspielraum.[702]

---

697 A.A. *Ziebarth*, Onlinedurchsuchung, S. 195.

698 Vgl. OVG-Vermerk 1120-13-1 zum Schutz des Kernbereichs privater Lebensgestaltung, S. 3.

699 I.E. auch OVG-Vermerk 1120-13-1 zum Schutz des Kernbereichs privater Lebensgestaltung, S. 3. Ob man dieses Ergebnis wie das OVG aus einer restriktiven Interpretation der Gewaltenteilung und der Vorbefassung des OVG als Institution ableiten mag, kann daher dahinstehen.

700 Vgl. *Schenke*, POR, Rn. 102; Rachor, in: Lisken/ Denninger, Handbuch, Kap. E, Rn. 105.

701 Vgl. BVerfG NJW 2013, 1499, 1510.

702 Vgl. dazu *Sodan/ Ziekow*, Grundkurs, § 68 Rn. 4 ff.

3.3.10.4.2 Gewaltenteilung und Aufgabe der Rechtsprechung

Sachleitungsbefugnis bedeutet im Wesentlichen die Herrschaft über ein bestimmtes Verfahren oder einen Verfahrensabschnitt. Die Vorbereitung und Durchführung der polizeirechtlichen Wohnraum- und Telekommunikationsüberwachung und die Online-Durchsuchung stellen Aufgaben der Gefahrenabwehrbehörde dar. Diese gehören der Exekutive an. Auch die Durchsicht der Daten auf Kernbereichsrelevanz obliegt zwei Bediensteten der Polizeibehörde sowie dem behördlichen Datenschutzbeauftragten und ist demnach dem Bereich der Exekutive zuzuordnen. Unter diesen Umständen ist es problematisch, die Sachleitungsbefugnis dem OVG, also einem Organ der Judikative, zuzuweisen.[703] Das Prinzip der Gewaltenteilung ergibt sich aus Art. 92, 20 Abs. 2 S. 2 GG.[704] Darin heißt es: „Die rechtsprechende Gewalt ist den Richtern anvertraut." Das BVerfG hat bislang keine allgemeingültige Definition der „Rechtsprechung" im Sinne des Art. 92 GG getroffen. Fest steht, dass der Begriff nicht nur rein formell bestimmt wird, sondern auch nach materiellen Kriterien. [705] Das BVerfG hat drei Fallgruppen entwickelt:[706]

- Wenn das Grundgesetz selbst eine Aufgabe den Gerichten oder Richtern überträgt, etwa über Rechtswegzuweisungen oder durch konkrete Richtervorbehalte.[707] Dazu gehören auch Akte der öffentlichen Gewalt, gegen die nach Art. 19 Abs. 4 GG die Gerichte zuständig sind.[708] Dadurch wird etwa die Verwaltungsgerichtsbarkeit begründet.
- Wenn es sich um einen traditionell anerkannten Aufgabenbereich handelt, so die bürgerliche Rechtspflege und die Strafrechtspflege.[709]

---

703 Vgl. OVG-Vermerk 1120-13-1 zum Schutz des Kernbereichs privater Lebensgestaltung, S. 4.

704 Vgl. *Hillgruber*, in: Maunz/ Dürig, GG, Art. 92 Rn. 13.

705 Vgl. BVerfG NJW 1967, 1219; BVerfG NJW 1988, 405, 406; kritisch zum Umgang des BVerfG mit dem formellen und materiellen Rechtsprechungsbegriff vgl. *Maunz/ Dürig*, GG, Art. 92 Rn. 32.

706 Vgl. *Morgenthaler*, in: Epping/ Hillgruber, GG, Art. 92 Rn. 6 ff.

707 Vgl. BVerfG NJW 1967, 1219.

708 Vgl. *Hillgruber*, in: Maunz/ Dürig, Art. 92 Rn. 33. Auch richterliche Anordnungen gehören dazu, vgl. oben und *Jarass*, in: Jarass/ Pieroth, GG, Art. 19 Rn. 45; BVerfG NJW 2003, 1924, 1925.

709 Vgl. BVerfG NJW 1967, 1219, 1220.

– Wenn dem Richter durch Gesetz Aufgaben zugewiesen werden, die nicht oder nicht ohne weiteres zu den regelmäßigen typischen Aufgaben der Gerichte gehören.[710]

Für die Sachleitungsbefugnis in § 39a Abs. 4 POG kommt nur die dritte Fallgruppe in Betracht. Die gesetzliche Zuweisung ist von bestimmten Voraussetzungen abhängig:[711]

– Die einfachgesetzliche Qualifizierung einer Tätigkeit als Rechtsprechung scheidet aus, wenn das Grundgesetz die Wahrnehmung der betreffenden Aufgabe einer anderen Gewalt vorbehält.[712]

– Es darf durch eine allzu weitgehende Belastung mit justizfremden Aufgaben die Leistungsfähigkeit der Dritten Gewalt in ihrem eigentlichen, verfassungsrechtlich vorgegebenen Aufgabenbereich nicht beeinträchtigt werden.[713]

– Aus dem Gewaltenteilungsgrundsatz folgt, dass den Gerichten keine wesentlichen, geschweige denn sämtliche Verwaltungsangelegenheiten übertragen werden dürfen. Es muss mit anderen Worten neben dem gerichtlichen auch noch verwaltungsbehördlichen Gesetzesvollzug geben.

– Entschließt sich der Gesetzgeber dazu, eine gerichtliche Zuständigkeit für die Wahrnehmung bestimmter Aufgaben, die materiell keine Rechtsprechung im Sinne des Art. 92 GG darstellen, in rechtsprechender Funktion zu begründen, so muss das darauf bezogene Verfahren mit allen verfassungsrechtlichen Garantien des gerichtlichen Verfahrens ausgestattet sein.[714]

So wurde es als zulässig angesehen, Angelegenheiten der freiwilligen Gerichtsbarkeit – selbst wenn sie nicht Rechtsprechung im traditionellen Sinn darstellen sollte – den Zivilgerichten zuzuweisen.[715]

Da die Sachleitungsbefugnis des OVG in Rheinland-Pfalz und im BKAG sowohl im Bereich des Gefahrenabwehrrechts als auch der Strafverfolgung ein

---

710 Vgl. BVerfG NJW 1983, 2812.

711 Vgl. *Hillgruber*, in: Maunz/ Dürig, GG, Art. 92 Rn. 58 f.

712 Vgl. BVerfG NJW 1983, 2812.

713 Vgl. BVerfG NJW 1958, 97, 98.

714 Vgl. *Hillgruber*, in: Maunz/ Dürig, GG, Art. 92 Rn. 60; BVerfG NJW 1967, 1219, 1220.

715 Vgl. BVerfG NJW 1967, 1123.

Novum darstellt, ist Rechtsprechung dazu noch nicht vorhanden. Nach unserem Dafürhalten gehört die Sachleitungsbefugnis des § 39a Abs. 3 POG insoweit zur rechtsprechenden Gewalt im Sinne des Art. 92 GG und verstößt nicht gegen die Gewaltenteilung.[716] Die ersten drei oben genannten Voraussetzungen für die gesetzliche Zuweisung der Aufgabe an das OVG sind erfüllt. Für die vierte Voraussetzung obliegt es dem Gericht selbst, verfahrensrechtliche Vorkehrungen zu treffen.

Im Einzelnen:

- Eine grundrechtliche Bestimmung bezüglich der zu evaluierenden Normen, die eine andere Gewalt für zuständig erklären würde, besteht nicht. Das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme nach Art. 1 Abs. 1, Art. 2 Abs. 1 GG, das Fernmeldegeheimnis nach Art. 10 GG sehen keine Zuordnung der Aufgaben an eine bestimmte Gewalt vor. Art. 13 Abs. 3 und 4 GG sehen einen Richtervorbehalt für Maßnahmen vor, die in das Wohnungsgrundrecht eingreifen. Art. 13 Abs. 5 GG erklärt lediglich, dass die Maßnahme „durch eine gesetzlich bestimmte Stelle angeordnet werden“ kann. Richterliche Entscheidungen sind auch insoweit nicht ausgeschlossen.[717]
- Die Sachleitungsbefugnis stellt keine wesentliche Verwaltungstätigkeit dar. Sie ist auch nicht geeignet, den verwaltungsbehördlichen Gesetzesvollzug in entscheidendem Maße zu verdrängen: § 39a Abs. 4 POG verweist auf Maßnahmen, die bislang sowohl im Strafrecht als auch im Gefahrenabwehrrecht nur selten angewendet wurden (s.o.). Grund hierfür sind insbesondere die hohen verfassungsrechtlichen Anforderungen, die eine hohe Praxistauglichkeit verhindern.[718] Zudem obliegt die Prüfung der kernbereichsrelevanten Daten zwei Bediensteten der Polizeibehörde und dem behördlichen Datenschutzbeauftragten. Eine einschneidende Verschiebung in Richtung Dritte Gewalt liegt somit nicht vor. Die Sachleitungsbefugnis dient vielmehr dazu, den Grundrechtsschutz effektiv zu verstärken. Denn der Richter muss von sich aus Vorgaben machen und deren Umsetzung überprüfen.
- Die verfahrensrechtlichen Garantien der Sachleitung sind wie der Begriff selbst durch Auslegung zu ermitteln (zur Sachleitung s.o.).

---

716 A.A. *Würtenberger*, in: Ehlers/ Fehling/ Pünder, Verwaltungsrecht 3, § 69 Rn. 41.

717 Vgl. etwa *Fink*, in: Epping/ Hillgruber, GG, Art. 13 Rn. 23.

718 Vgl. auch *Aschmann*, Richtervorbehalt, S. 163.

3.3.10.4.3 Für den Kernbereichsschutz geeignetes Verfahren

Speziell für die Online-Durchsuchung in § 20k Abs. 7 BKAG und Art. 34d Abs. 4 BayPAG wird bestritten, dass die Sachleitungsbefugnis und die Durchsicht der Daten verfassungskonform seien.[719] Im Urteil des BVerfG heißt es dazu:

> *„Entscheidende Bedeutung für den Schutz hat insoweit die Durchsicht der erhobenen Daten auf kernbereichsrelevante Inhalte, für die ein geeignetes Verfahren vorzusehen ist, das den Belangen des Betroffenen hinreichend Rechnung trägt.“*[720]

Der sachleitende Richter sei durch die richterliche Anordnung bereits vorbefasst, die an der Durchsicht beteiligte Ermittlungsbehörde habe ein Eigeninteresse an den Ermittlungsergebnissen.[721] Dasselbe Problem ergibt sich für die richterlichen Anordnungen, soweit das OVG erst- und letztinstanzlich tätig wird. Da in Rheinland-Pfalz das OVG als Verwaltungsgericht zuständig ist, tritt eine Vorbefassung nicht ein. Die Sondervorschrift des § 54 Abs. 2 VwGO verbietet die Mitwirkung des Richters am vorausgegangenen Verwaltungsverfahren. Die Vorschrift wird weit verstanden. Der Begriff des Verwaltungsverfahrens geht über das Verfahren nach § 9 VwVfG hinaus und umfasst sämtliches Verwaltungshandeln.[722] Als „vorausgegangenes“ Verwaltungsverfahren ist das gesamte behördliche Verfahren anzusehen, in dem die nunmehr zur gerichtlichen Überprüfung gestellte Verwaltungsentscheidung ergangen ist.[723] Es genügt, dass sich der Richter in seiner früheren amtlichen Eigenschaft mit der

---

719 Vgl. *Petri*, in: Lisken/ Denninger, Handbuch, Kap. G, Rn. 360.

720 Vgl. BVerfG NJW 2008, 822, 834, Rn. 283.

721 Vgl. *Petri*, in: Lisken/ Denninger, Handbuch, Kap. G, Rn. 360; *Sandkuhl*, Stellungnahme DAV, S. 17; kritisch auch OVG-Vermerk 1120-13-1 zum Schutz des Kernbereichs privater Lebensgestaltung, S. 4; vgl. auch das Vorbringen der gegen das BKAG erhobenen Beschwerde (Urteil v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09, Rn. 30): „§ 20k Abs. 7 S. 3, 4 BKAG werde der gebotenen Durchsicht der erhobenen Daten durch eine unabhängige Stelle nicht gerecht; als eine solche komme grundsätzlich nur ein Gericht in Frage. An der Sichtung nach § 20k Abs. 7 S. 3, 4 BKAG würden aber im Wesentlichen Personen des Bundeskriminalamts beteiligt. Was unter der vorgesehenen „Sachleitung“ des anordnenden Gerichts zu verstehen sei, bleibe unklar; sie sichere die Unabhängigkeit der Sichtung nicht.“

722 Vgl. *Kimmel*, in: Posser/ Wolff, VwGO, § 54 Rn. 20; *Krausnick*, in: Gärditz, VwGO, § 54 Rn. 23; *Czybulka*, in: Sodan/ Ziekow, VwGO, § 54 Rn. 36.

723 Vgl. *Kimmel*, in: Posser/ Wolff, VwGO, § 54 Rn. 21.

Sache befasst hat.[724] Selbst wenn die Zivilgerichte zuständig wären, verfinge der Einwand des möglicherweise befangenen Richters grundsätzlich nicht. In der Rechtsprechung ist anerkannt, dass die Mitwirkung an Zwischenentscheidungen im anhängigen Verfahren für eine Ablehnung desselben Richters, der in der Hauptsache entscheidet, nicht hinreichend ist.[725] „Das deutsche Verfahrensrecht wird von der Auffassung beherrscht, dass der Richter auch dann *unvoreingenommen* an die Beurteilung einer Sache herantritt, wenn er sich schon früher über denselben Sachverhalt ein Urteil gebildet hat.“[726]

Für die richterliche Anordnung müssen daher andere Richter zuständig sein als für die Aufgabe der Sachleitung.

3.3.10.4.4 Durchsicht durch zwei Bedienstete und den Datenschutzbeauftragten

Die Durchsicht der Daten durch zwei Bedienstete der zuständigen Polizeibehörde und des behördlichen Datenschutzbeauftragten wird teils als ausreichend[727], teils als problematisch angesehen[728]. Es sei lebensfremd anzunehmen, dass das dadurch erlangte Wissen nicht verwendet werde.[729] Zumindest sei ein Interessenskonflikt gegeben, da die Behörde, welche die Daten erhoben hat, zugleich über deren Verwertung mitentscheide.[730] Mit dem Urteil des BVerfG zum BKAG und dessen Ablehnung der in § 20k Abs. 73 S. 3 geregelten und § 39a Abs. 4 S. 2 POG entsprechenden Kontrolle erscheint die Ausgestaltung der Durchsicht, wie sie § 39a Abs. 4 S. 2 POG vorsieht, änderungsbedürftig.

---

724 Vgl. *v. Albedyll*, in: Bader u.a., VwGO, § 54 Rn. 25; Kugele, VwGO, § 54 Rn. 7.

725 Vgl. *Gehrlein*, in: MüKo ZPO, § 42 Rn. 14; *Schmitt*, in: Meyer-Goßner/ Schmitt, StPO, § 24 Rn. 14; *Fischer*, in: KK-StPO, § 24 Rn. 8; *v. Albedyll*, in: Bader u.a., VwGO, § 54 Rn. 27 zu PKH und vorläufigem Rechtsschutz.

726 *Cirener*, in: Graf, StPO, § 24 Rn. 12.

727 Vgl. *Ruthig*, Kernbereich, S. 518.

728 Vgl. *Schneider*, Onlinedurchsuchung, S. 113; Zabel, JR 2009, 453, 457 zu § 20k BKAG; *Gusy*, DuD 2012, 33, 40; BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09, 1140/09, Rn. 224.

729 Vgl. *Bäcker*, BKA, S. 90; Hornung, DuD 2007, 575, 577.

730 Vgl. *Kulwicki*, Verfassungswandel, S. 68 zu § 20k BKAG; *Bäcker*, IT-Grundrecht, S. 29 zu § 20k BKAG; *Würtenberger*, in: Ehlers/ Fehling/ Pünder, Verwaltungsrecht 3, § 69 Rn. 41.

Das BVerfG betont die notwendige Wirksamkeit[731] und Unabhängigkeit[732] der Sichtung, weshalb es jedenfalls für die Online-Überwachung die Mitwirkung (maximal) *eines*[733] durch gesonderte Verschwiegenheitspflichten abgesicherten Bediensteten des BKA zwecks Gewährleistung ermittlungsspezifischen Sachverstandes,[734] erlaubt und fordert, dass die tatsächliche Durchführung und Entscheidungsverantwortung maßgeblich in den Händen dem BKA gegenüber unabhängiger Personen liegen müsse[735]. Dies sei durch die Kontrolle durch zwei BKA-Beamten und einen behördlichen Datenschutzbeauftragten unter Sachleitung des anordnenden Gerichts nicht gegeben.[736]

3.3.11 Schutz von Berufsgeheimnisträgern (§ 39b POG)

3.3.11.1 Erhebungs- und Verwertungsverbot, Löschungs- und Dokumentationspflicht (§ 39b Abs. 1 POG)

Als problematisch an der Regelung in Rheinland-Pfalz angesehen wird teilweise, dass zwischen den einzelnen Berufsgruppen nicht differenziert wird.[737] Zu der für die Strafverfolgung entsprechenden Vorschrift des § 160a StPO führt das BVerfG aus: [738]

> „Die Normierung eines absoluten Beweiserhebungs- und -verwendungsverbotes in § 160 a Abs. 1 StPO beschränkt die Strafverfolgung in erheblichem Maße, weil sie in Anknüpfung an die Zugehörigkeit zu bestimmten Berufsgruppen Ermittlungsmaßnahmen von

731 BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BVR 1140/09, Rn. 141.

732 BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BVR 1140/09, Rn. 129, 204, 220, 224, 241.

733 Kursiv hervorgehoben in BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09, 1 BVR 1140/09, Sondervotum Schluckebier, Rn. 14.

734 BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BVR 1140/09, Rn. 224 zu § 20k BKAG (Online-Durchsuchung).

735 BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BVR 1140/09, Rn. 224 zu § 20k BKAG (Online-Durchsuchung).

736 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BVR 1140/09, Rn. 224, 225 zu § 20k BKAG (Online-Durchsuchung).

737 Kritisch dazu *Rühle*, POG, Kap. G, Rn. 78, 97.

738 Vgl. BVerfG NJW 2012, 833, 842, Rn. 257.

> vornherein untersagt und jede Verwendung dennoch erlangter Erkenntnisse unterbindet. Derartige absolute Verbote können nur in engen Ausnahmefällen (Hervorh. d. Verf.) zum Tragen kommen, insbesondere wenn eine Ermittlungsmaßnahme mit einem Eingriff in den Schutzbereich der Menschenwürde verbunden wäre, die jeder Abwägung von vornherein unzugänglich ist. Nur in solchen Fällen ist es zulässig – und unter Umständen auch verfassungsrechtlich geboten –, bereits eine Beweiserhebung generell zu untersagen und jede Verwendung gleichwohl erlangter Erkenntnisse auszuschließen."

Die zitierte Entscheidung des BVerfG kann auch für das Gefahrenabwehrrecht fruchtbar gemacht werden. Dem grundrechtlichen Schutz von Berufsfreiheit und Menschenwürde steht insoweit das öffentliche Interesse an einer effektiven Gefahrenabwehr gegenüber. Das BVerfG hat in dieser Entscheidung allerdings nur geprüft, ob aufgrund Art. 3 Abs. 1 GG bestimmte Berufsgruppen nicht auch in den absoluten Schutz des § 160a Abs. 1 StPO aufgenommen werden müssen.[739] Die Frage, ob auch andere Berufsgruppen in den Schutz aufgenommen werden *dürfen*, war nicht Gegenstand der Entscheidung.[740] Allerdings deuten die vom BVerfG bereits zitierten allgemein gemachten Ausführungen darauf hin, dass dem Gesetzgeber ein absoluter Schutz von Berufsgeheimnisträgern verwehrt ist. Das Landesgesetz wäre also entsprechend zu ändern. Das abgestufte Schutzkonzept[741] mit einem – vom Gesetzgeber als besonders schutzbedürftig betrachteten – strikt geschützten Personenkreis in § 160a Abs. 1 StPO und § 20u Abs. 1 BKAG sowie einem nur nach Maßgabe einer Abwägung geschützten Personenkreis in § 160a Abs. 2 StPO und § 20u Abs. 2 BKAG ist nach Auffassung des BVerfG verfassungsgemäß[742]. Die in § 160a Abs. 2 S. 1 Halbs. 2 StPO enthaltene Direktive, dass von einem Überwiegen der Interessen der Sicherheitsbehörde an der Datenerhebung nicht auszugehen sei, wenn die Maßnahme nicht der Abwehr einer erheblichen Gefahr diene, ist nach dem BVerfG auch im Rahmen einer Abwägung nach Maßgabe des

---

739 Offen gelassen von ThürVerfGH, Urt. v. 21.11.2012 – 19/09.

740 So prüft das BVerfG, ob eine Pflicht besteht, Pressevertreter in den absoluten Schutz einzubeziehen und ob der relative Schutz nach § 160a Abs. 2 StPO für andere Berufsgruppen gerechtfertigt ist, vgl. BVerfG, NJW 2012, 833, 843, Rn. 267 ff. Ein Anspruch für Medienvertreter auf strikteren Schutz wird vom BVerfG verneint, vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09, Rn. 258.

741 Vgl. *Kugelmann*, BKA-Gesetz, § 20u Rn. 2.

742 BVerfG, NJW 2012, 833 f., Rn. 247 (zu § 160 a StPO); BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09, Rn. 256 (zu § 20u BKAG).

§ 20u Abs. 2 BKAG anzuwenden[743]. Ungeeignet und verfassungsrechtlich nicht tragfähig wäre nach Auffassung des BVerfG, im Gefahrenabwehrrecht zwischen Strafverteidigern und in anderen Rechtsverhältnissen tätigen Rechtsanwälten zu unterscheiden, weil die entsprechenden Überwachungsmaßnahmen nicht der Strafverfolgung, sondern der Gefahrenabwehr dienen.[744]

Gefordert wird teilweise, der Berufsgruppe der Steuerberater auch einen absoluten Berufsgeheimnisschutz zu gewähren. Ebenso wie für Rechtsanwälte sei auch für Steuerberater der Übergang von der Beratung zur absolut geschützten Strafverteidigung fließend.[745] Beide seien Organe der (Steuer-)Rechtspflege.[746] In einer neueren Entscheidung hat das BVerfG allerdings die Differenzierung zwischen absolut geschützten Rechtsanwälten und relativ geschützten Steuerberatern für verfassungskonform erachtet.[747]

3.3.11.2 Für die Gefahr verantwortliche Personen (§ 39b Abs. 2 POG)

Das BVerfG hat die entsprechende Verstrickungsregelung[748] des § 160a Abs. 4 StPO für verfassungskonform erachtet.[749] Danach können sich Personen nicht auf den Schutz des Berufsgeheimnisträgers nach §§ 53, 53a StPO berufen, wenn „bestimmte Tatsachen den Verdacht begründen, dass die zeugnisverweigerungsberechtigte Person an der Tat oder an einer Begünstigung, Strafvereitelung oder Hehlerei beteiligt ist.“ Das Merkmal der „bestimmten Tatsachen“ erfordert eine konkretisierte Verdachtslage[750]. Zwar findet sich in § 39b Abs. 2 POG nur der Begriff der Tatsachen, nicht aber der bestimmten

---

743 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09, Rn. 256. Vgl. dazu auch Wittmann, AnwBl 2016, 497.

744 Vgl. BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09, Rn. 257.

745 Vgl. *Vinken*, DStR-KR 2012, 5; *Schmidt-Keßeler*, DStR 2011, 1586; vgl. auch *Ende*, DStR 2009, 2556, 2559; Anmerkung *Kalina-Kerschbaum*, DStR 2012, 537, 538.

746 Vgl. § 1 BRAO, § 1 BOStB.

747 Vgl. BVerfG NJW 2012, 833, 842.

748 Siehe z.B. *Zöller*, in Gercke u.a., StPO, § 160a, Rn. 17; im Gefahrenabwehrrecht: LT-Drs. 15/4879, S. 45; *Roos/Lenz*, POG, § 39b Rn. 2 und z.B. BT-Drs. 16/10121, S. 36 zu § 20u Abs. 4 BKAG.

749 Vgl. BVerfG NJW 2012, 833, 843.

750 BVerfG NJW 2012, 833, 843, Rn. 273.

Tatsachen. Das BVerfG hat eine solche Formulierung jedoch anderweitig mit der Verfassung für vereinbar erklärt.[751]

Ein absoluter Schutz der Berufsgeheimnisträger auch für den Fall, dass sie an der Tat beteiligt oder für die Gefahr verantwortlich sind, dürfte dem Interesse an effektiver Strafverfolgung bzw. Gefahrenabwehr entgegenstehen und wäre demnach verfassungswidrig.[752] Eine Kollision mit möglicherweise einer Datenerhebung entgegenstehendem höherrangigem Recht ist nicht zu befürchten, da trotz Entfallen der Schutzvorschriften, weiterhin der Grundsatz der Verhältnismäßigkeit zu beachten ist, insbesondere ob die Intensität der Gefahr und die Bedeutung der bedrohten Rechtsgüter in einem angemessen Verhältnis zu dem Gewicht der Grundrechtsbeeinträchtigung stehen[753].

3.3.12 Pflicht zur Benachrichtigung Betroffener (§ 40 Abs. 5, 6 POG)

Im Gegensatz zu § 40 Abs. 6 POG war § 40 Abs. 5 POG seit seiner Einfügung im Jahre 2004 mehrmals Gegenstand gesetzgeberischer Änderungen. Ausweislich der jeweiligen Begründungen hierzu dienten die Änderungen jeweils der Anpassung der Vorschrift an Vorgaben des Bundesverfassungsgerichts.[754]

3.3.12.1 Betroffene Grundrechte, insbesondere Art. 19 Abs. 4 GG

Der Anspruch der von einer heimlichen Überwachungsmaßnahme Betroffenen auf Benachrichtigung hierüber ergibt sich aus der Rechtsweggarantie des

751 Vgl. BVerfG NJW 2004, 2213, 2217 zu § 39 AWG a.F.

752 Vgl. BVerfG NJW 2012, 833, 843; ThürVerfGH, Urt. v. 21.11.2012 – 19/09, Ziff. II 5 c) bb); vgl. auch *Shirvani*, VerwArch 2010, S. 86, 110.

753 Vgl. *Ruthig*, in: Schenke/ Graulich/ Ruthig, Sicherheitsrecht des Bundes, § 20u BKAG, Rn. 19 mit Verweis u.a. auf die Entscheidung des BVerfG, NJW 2012, 833, 843, Rn. 273 zu § 160a Abs. 4 StPO.

754 So schon die Begründung zur Ursprungsfassung des § 40 Abs. 5 POG, Landesregierung, LT-Drs. 14/2287, S. 53; zu den Änderungen: Fraktionen der SPD und FDP, LT-Drs. 14/3936, S. 11 f. Lediglich die jüngste Änderung des § 40 Abs. 5 POG wird nicht mehr explizit auf ein Urteil des BVerfG zurückgeführt, Landesregierung, LT-Drs. 15/4879, S. 45.

Art. 19 Abs. 4 GG in Verbindung mit dem Grundrecht, in das durch die Überwachungsmaßnahme eingegriffen wurde.[755] Die Rechtsschutzgarantie des Art. 19 Abs. 4 GG ist nicht ausschließlich auf gerichtlichen Rechtsschutz beschränkt, sondern kann auch eine Benachrichtigung der von der Maßnahme Betroffenen gebieten, wenn die Kenntnis von der Maßnahme „Voraussetzung der Inanspruchnahme gerichtlichen Rechtsschutzes ist".[756] Hinzu kommt, dass die Kenntnis von der Maßnahme auch die Voraussetzung für die Geltendmachung weiterer Rechte, wie z.B. auf Löschung der erhobenen Daten ist.[757] Regelungen über die Benachrichtigung der von einer nicht offen erfolgenden Datenerhebung Betroffenen stellen elementare Instrumente des grundrechtlichen Datenschutzes dar.[758] Ein Absehen von der nachträglichen Benachrichtigung über die durchgeführten Maßnahmen ist von Verfassungs wegen nicht grundsätzlich verboten, stellt aber selbst wiederum einen Eingriff in die Grundrechte dar,[759] so dass „die jeweils betroffenen Grundrechte und ihre Schranken in den Blick zu nehmen" sind.[760]

3.3.12.2 Grundsätze der Benachrichtigungspflicht (§ 40 Abs. 5 S. 1-3 POG)

§ 40 Abs. 5 S. 1 POG legt zunächst den Grundsatz fest, dass jeder, gegen den sich eine verdeckte Datenerhebung richtet, nach Abschluss der Maßnahme hierüber zu unterrichten ist. Dies steht mit den vom BVerfG entwickelten Grundsätzen im Einklang: Demnach gebietet es die Verfassung, dass eine Benachrichtigung immer in den Fällen stattfindet, in denen die Datenerhebung

---

755 BVerfG, Urt. v. 12.10.2011 – 2 BvR 236/08, Rn. 182; BVerfGE 125, 260, 336; BVerfG, NJW 2004, 999, 1015 f. zu Art. 13 GG); BVerfG, Urt. v. 14.07.1999 – 1 BvR 2226/94 u.a., Rn. 181 (zu Art. 10 GG); ThürVfGH, Urt. v. 21.11.2012 – 19/09, Rn. 268; *Petri,* in: Lisken/ Denninger, Handbuch, Kap. G, Rn. 52. Die Begründung zum ursprünglichen § 40 Abs. 5 S. 1 POG geht konsequenterweise auch von einer entsprechenden Rechtspflicht der Polizei aus, Landesregierung, LT-Drs. 14/2287, S. 53.

756 BVerfG, Urt. v. 14.07.1999 – 1 BvR 2226/94 u.a., Rn. 181; BVerfGE 65, 1, 70; ähnlich BVerfG, Urt. v. 12.10.2011 – 2 BvR 236/08, Rn. 194.

757 BVerfG, Urt. v. 12.10.2011 – 2 BvR 236/08, Rn. 226; BVerfG NJW 2004, 999, 1015; BVerfG, NVwZ 2001, 1261, 1263; *Petri*, in: Lisken/ Denninger, Handbuch, Kap. G, Rn. 52; Landesregierung, LT-Drs. 14/2287, S. 53; *Roos/ Lenz*, POG, § 40 Rn. 11.

758 BVerfG, Urt. v. 12.10.2011 – 2 BvR 236/08, Rn. 226; BVerfGE 125, 260, 335.

759 BVerfG, Urt. v. 14.07.1999 – 1 BvR 2226/94 u.a., Rn. 181; BVerfG, NJW 2004, 999, 1015 f. zu Art. 13 GG; Urt. v. 14.07.1999 – 1 BvR 2226/94 u.a., Rn. 181; ThürVfGH, Urt. v. 21.11.2012 – 19/09, Rn. 269.

760 ThürVfGH, Urt. v. 21.11.2012 – 19/09, Rn. 273.

heimlich erfolgt ist und Auskunftsansprüche nicht eingeräumt wurden oder den Rechten der Betroffenen nicht angemessen Rechnung getragen haben.[761]

Fraglich scheint hingegen, ob auch Satz 2 des § 40 Abs. 5 POG den verfassungsrechtlichen Anforderungen gerecht wird. Nach dieser Vorschrift sind sonstige betroffene Personen nur zu unterrichten, soweit die Datenerhebung nach §§ 29, 31c POG erfolgt ist oder andere besonders schutzwürdige Interessen dies erfordern. Von besonders schutzwürdigen Interessen ging der Gesetzgeber bei dem insoweit inhaltsgleichen § 40 Abs. 5 S. 3 POG a.F. aus, wenn ein besonders geschütztes Vertrauensverhältnis berührt wird.[762] Auch wenn die Benachrichtigungspflicht grundsätzlich gegenüber allen von der Datenabfrage Betroffenen, also sowohl gegenüber dem Beschuldigten, dem Polizeipflichtigen als auch gegenüber dem Dritten, gilt,[763] ist es nach Ansicht des Bundesverfassungsgerichts dennoch verfassungsrechtlich nicht geboten, „vergleichbar strenge Benachrichtigungspflichten gegenüber Personen zu begründen, die nur zufällig von einer Ermittlungsmaßnahme gegen einen Beschuldigten betroffen sind und somit nicht Ziel des behördlichen Handelns sind.“[764] Solchermaßen zufällig Betroffene kann es nach Ansicht des Gerichts in großem Umfang geben, „ohne dass das kurzfristige Bekanntwerden ihrer Daten Spuren hinterlässt oder Folgen für den Betroffenen haben muss. Eine Benachrichtigung kann ihnen gegenüber im Einzelfall den Eingriff vielmehr vertiefen. In diesen Fällen kann eine Benachrichtigung grundsätzlich schon dann unterbleiben, wenn die Betroffenen von der Maßnahme nur unerheblich betroffen wurden und anzunehmen ist, dass sie kein Interesse an der Benachrichtigung haben.[765] Einer richterlichen Bestätigung dieser Abwägungsentscheidung bedarf es nicht“;[766] sie kann beispielsweise der Staatsanwaltschaft überlassen bleiben.[767]

---

761 BVerfG, Urt. v. 14.07.1999 – 1 BvR 2226/94 u.a., Rn. 172; BVerfG, NJW 2004, 999, 1016.

762 Landesregierung, LT-Drs. 14/2287, S. 53.

763 BVerfGE 125, 260, 336; explizit für das Beispiel der Wohnraumüberwachung: BVerfG, NJW 2004, 999, 1016.

764 BVerfG, Urt. v. 12.10.2011 – 2 BvR 236/08, Rn. 227; BVerfGE 125, 260, 337; BVerfG, Urt. v. 14.07.1999 – 1 BvR 2226/94 u.a., Rn. 227;

765 BVerfG, Urt. v. 12.10.2011 – 2 BvR 236/08, Rn. 226; BVerfGE 125, 260, 337.

766 BVerfG, Urt. v. 12.10.2011 – 2 BvR 236/08, Rn. 231 f.; BVerfGE 125, 260,337.

767 BVerfG, Urt. v. 12.10.2011 – 2 BvR 236/08, Rn. 231.

Eine Abwägung sieht § 40 Abs. 5 S. 2 POG aber gerade nicht vor; im Fall der Wohnraumüberwachung, der Online-Durchsuchung sowie bei Betroffenheit besonders schutzwürdiger – aber anders als in § 20w Abs. 2 S. 3 BKAG oder § 101 Abs. 4 S. 3 StPO nicht mit dem Attribut (d.h. gegenüber dem Interesse von anderen Betroffenen an dem Unterbleiben der Benachrichtigung) „überwiegend“ beschriebener – Interessen sind sonstige Betroffene vielmehr zu informieren, unabhängig davon, ob hierdurch z.B. der Grundrechtseingriff für die Zielperson verstärkt wird, weil die Überwachung ergebnislos geblieben ist oder weil die Betroffenen bislang unbekannt geblieben sind und die Feststellung ihrer Identität weitere Grundrechtseingriffe notwendig macht.[768] In diesen Fällen ist nach Ansicht des BVerfG eine Abwägungsentscheidung erforderlich, in die neben der Intensität des Grundrechtseingriffs auch der Aufwand für die Feststellung der Identität der Betroffenen sowie die Beeinträchtigungen, die sich hierdurch sowohl für die Zielperson als auch für sonstige Beteiligte ergeben können, eingestellt werden müssen.[769] Auf der anderen Seite verzichtet § 40 Abs. 5 POG darauf, eine Benachrichtigungspflicht auch für solche Betroffene zu normieren, die außerhalb der §§ 29, 31c POG keine besonders schutzwürdigen Interessen an der Benachrichtigung geltend machen können.[770] Insoweit werden die Voraussetzungen, wonach eine Benachrichtigung ausnahmsweise unterbleiben kann, wenn anzunehmen ist, dass der Betroffene kein Interesse daran hat, quasi in ihr Gegenteil verkehrt, wenn das Vorliegen besonders schutzwürdiger Interessen zur Voraussetzung der Benachrichtigung gemacht wird. Somit gestaltet § 40 Abs. 5 S. 2 POG einerseits die Benachrichtigungspflicht zu streng aus, wenn keine Abwägungsmöglichkeit im Einzelfall eröffnet wird, die ein Absehen von der Benachrichtigung der von einer Maßnahme nach §§ 29, 31c POG Betroffenen oder der Betroffenen, die ein besonders schutzwürdiges Interesse an der Benachrichtigung haben, für die allerdings über die Auslegung des Begriffs „schutzwürdig“ ein Raum für gleichwohl nicht näher definierte Abwägungen bestehen könnte, ermöglicht; dabei kann insbesondere nicht auf den Ausschlussgrund des § 40 Abs. 6 Nr. 2 POG verwiesen werden, da hier keine Abwägung mit den Interessen der eigentlichen Zielperson vorgesehen ist. Diese Vorschrift stellt alleine auf das Interesse der sonstigen betroffenen Person ab.[771] Andererseits ist die Vorschrift

768 So explizit zur Wohnraumüberwachung BVerfG, NJW 2004, 999,1016.

769 BVerfG, NJW 2004, 999,1016.

770 So ausdrücklich auch Fraktionen der SPD und FDP, LT-Drs. 14/3936, S. 11.

771 So ist wohl auch die Gesetzesbegründung zu verstehen, vgl. Landesregierung, LT-Drs. 14/2287, S. 53 f.

nicht weitreichend genug, soweit sonstige Betroffene, deren Daten nicht im Rahmen einer Maßnahme nach §§ 29, 31c POG erhoben wurden oder die kein besonders schutzwürdiges Interesse geltend machen können, grundsätzlich nicht benachrichtigt werden müssen. Denn auch solche „nur" einfach Betroffene haben unter verfassungsrechtlichen Gesichtspunkten grundsätzlich ein Recht auf nachträgliche Benachrichtigung von der heimlichen Datenerhebung.

Aus den oben genannten Gründen ist festzustellen, dass § 40 Abs. 5 S. 2 POG den verfassungsrechtlichen Anforderungen nicht genügt; auch eine verfassungskonforme Auslegung scheidet angesichts des eindeutigen Wortlauts der Vorschrift aus. Ein von der Verfassungsgerichtsbarkeit gebilligtes System von Ausnahmen zur Benachrichtigungspflicht, findet sich in § 20w BKAG[772] und § 101 Abs. 4-6 StPO[773]. Die Benachrichtigung primär und sekundär Betroffener[774] unterbleibt gemäß § 20w Abs. 1 S. 2 BKAG und § 101 Abs. 4 S. 3 StPO zwingend, wenn ihr überwiegende schutzbedürftige Belange einer betroffenen Person entgegenstehen. Ein Absehen von der Benachrichtigung der Zielperson wird dabei nur in besonderen Fällen in Betracht kommen.[775] Bei bestimmten Arten von Überwachungsmaßnahmen[776], kann gemäß § 20w Abs. 1 S. 3 BKAG und § 101 Abs. 4 S. 4 StPO im Ermessen der Behörde[777] die Benachrichtigung unterbleiben, wenn die Person von der Maßnahme nur unerheblich betroffen wurde und anzunehmen ist, dass sie kein Interesse an einer Benachrichtigung hat. Diese Regelung trägt dem Umstand Rechnung, dass von den in Bezug genommenen Maßnahmen zwar regelmäßig viele Personen in ihrem Grundrecht aus Art. 10 GG bzw. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG betroffen werden, dies aber im Einzelfall in einer vergleichsweise so geringfügigen Weise, dass ein Interesse an einer Benachrichtigung oftmals nicht anzunehmen ist.[778],

---

772 Vgl. BVerfG, Urt. v. 20.04.2016, Az. 1 BvR 966/09 und 1 BvR 1140/09, Rn. 260

773 Vgl. BVerfG, NJW, 2012, 833, 838-840, Rn. 225-242.

774 Vgl. *Kugelmann*, BKA-Gesetz, § 20w Rn. 3.

775 Vgl. BT-Drs. 16/10121, S. 38 zu § 20w BKAG.

776 Postbeschlagnahme (§ 101 Abs. 4 S. 1 Nr. 2, S. 3 StPO), Online-Durchsuchung (§ 20w Abs. 1 S. 1 Nr. 6, S. 3 BKAG), Telekommunikationsüberwachung (§ 101 Abs. 4 S. 1 Nr. 3, S. 3 StPO; § 20w Abs. 1 S. 1, Nr. 7, S. 3 BKAG); Erhebung von Verkehrsdaten (§ 20w Abs. 1 S. 1 Nr. 8, S. 3 BKAG).

777 Vgl. BVerfG NJW 2010, 833, 843, Rn. 245.

778 Vgl. BT-Drs. 16/10121, S. 38 zu § 20 w BKAG; BT-Drs. 16/5846, S. 59 zu § 101 Abs. 4 S. 4 StPO.

Gegen die Ordnungsvorschrift[779] von § 40 Abs. 5 S. 3 bestehen hingegen keine Bedenken.

3.3.12.3 Zeitlich befristete Zurückstellung der Benachrichtigung (§ 40 Abs. 5 S. 4 POG)

Da Verzögerungen in der Benachrichtigung von der heimlichen Datenerhebung Betroffenen bei der Wahrnehmung seiner datenschutzspezifischen Rechte (z.B. Löschung oder Berichtigung) beeinträchtigen können, „bedarf auch die zeitlich befristete Zurückstellung einer Benachrichtigung der verfassungsrechtlichen Rechtfertigung.“[780] Allerdings ist höchstrichterlich anerkannt, dass die Gefährdung der in § 40 Abs. 5 S. 4 POG genannten Rechtsgüter – Maßnahmezweck, Leib, Leben, Freiheit einer Person[781] sowie besondere Vermögenswerte[782] – das Recht auf Benachrichtigung überwiegen können.

3.3.12.4 Verfahrensrechtliche Absicherung der Ausnahmetatbestände (§ 40 Abs. 5 S. 5-9 POG)

§ 40 Abs. 5 S. 5 POG sieht für den Fall, dass auch ein Jahr nach Maßnahmeende eine Benachrichtigung aus den gesetzlichen Gründen unzulässig ist, eine richterliche Entscheidung vor: Die Benachrichtigung darf nur weiterhin zurückgestellt werden, wenn ein Richter zustimmt. Nach S. 6 der Norm gilt Entsprechendes nach Ablauf jeweils eines weiteren Jahres.

Diese Vorschriften sind verfassungsrechtlich nicht zu beanstanden. Sie tragen der Forderung Rechnung, dass eine regelmäßige, insbesondere bei langandauernder Zurückstellung nicht nur einmalige,[783] richterliche Überprüfung stattfindet, wenn zwingende Gründe die nachträgliche Benachrichtigung ausschließen.[784] Dabei wird die richterliche Überprüfung als Kompensation der

---

779 LT-Drs. 14/3936, S. 11; *Roos/ Lenz*, POG, § 40 Rn. 11.

780 ThürVfGH, Urt. v. 21.11.2012 – 19/09, Rn. 279.

781 BVerfG, NJW 2004, 999, 1016; BVerfGE 125, 260,336; ThürVfGH, Urt. v. 21.11.2012 – 19/09, Rn. 280.

782 BVerfG, NJW 2012, 833, 840 f., Rn. 234 ff.; ThürVfGH, Urt. v. 21.11.2012 – 19/09, Rn. 281.

783 BVerfG, NJW 2004, 999, 1016.

784 BVerfGE 125, 260, 335 ff.; BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 u. 1 BvR 1140/09, Rn. 136.

fehlenden Möglichkeit der persönlichen Interessenwahrnehmung durch die Betroffenen betrachtet.[785] Was die Festlegung der Zeitspanne der Zurückstellung anbelangt, nach deren Ablauf erstmalig eine richterliche Entscheidung notwendig wird, wird es als vom gesetzgeberischen Ermessen gedeckt angesehen, wenn die richterliche Entscheidung erstmalig nach Ablauf von zwölf Monaten vorgesehen wird.[786] Daneben „ist es von Verfassungs wegen nicht erforderlich, die Höchstdauer einer Zurückstellung gesetzlich vorzugeben. Der Gesetzgeber darf davon ausgehen, dass der Richter diese Dauer im Einzelfall unter Berücksichtigung aller relevanten Umstände festsetzt.“[787]

Die Zuständigkeitsregelungen der Sätze 7 und 8 des § 40 Abs. 5 POG begegnen ebenfalls keinen Bedenken. Vielmehr geht der rheinland-pfälzische Gesetzgeber sogar über das hinaus, was verfassungsrechtlich zu fordern ist: Durch die Zuständigkeitsregelung in Satz 8 wird noch einmal deutlich, dass eine richterliche Entscheidung in sämtlichen Fällen der nicht offenen Datenerhebung über die nach Satz 1 und 2 zu informieren ist, die nachträgliche Benachrichtigung aber zurückgestellt wird, einzuholen ist. Verfassungsrechtlich zwingend gefordert wird der Richtervorbehalt allerdings nur, wenn die heimliche Datenerhebung selbst einer richterlichen Anordnung bedurfte.[788]

Auch die Vorschrift zur Bestimmung des Fristbeginns in § 40 Abs. 5 S. 9 POG ist nicht zu beanstanden.

3.3.12.5 Ausnahmetatbestände (§ 40 Abs. 6 POG)

§ 40 Abs. 6 POG kennt drei (weitere) Ausnahmetatbestände. Eine Benachrichtigung unterbleibt demnach, wenn sich an den die Maßnahme auslösenden Sachverhalt ein strafrechtliches Ermittlungsverfahren gegen den Betroffenen anschließt (Nr. 1), wenn zu ihrer Durchführung weitere Daten über die betroffene Person erhoben werden müssten und dies im Interesse der betroffenen Person nicht geboten erscheint (Nr. 2) oder wenn keine Aufzeichnungen mit personenbezogenen Daten erstellt oder diese unverzüglich nach Beendigung der Maßnahme vernichtet worden sind (Nr. 3).

---

785 BVerfG, Urt. v. 12.10.2011 – 2 BvR 236/08, Rn. 194; BVerfG, NJW 2004, 999, 1016.

786 ThürVfGH, Urt. v. 21.11.2012 – 19/09, Rn. 289; Zwar sind für die Wohnraumüberwachung teilweise kürzere Fristen vorgesehen, z.B. sechs Monate nach § 101 Abs. 6 S. 5 StPO oder nach § 34 Abs. 11 S. 5 ThürPAG, doch dürfte dies nicht zwingend sein.

787 ThürVfGH, Urt. v. 21.11.2012 – 19/09, Rn. 289.

788 ThürVfGH, Urt. v. 21.11.2012 – 19/09, Rn. 277.

Diese Ausnahmetatbestände wurden bereits im Jahre 2004 normiert und sind – im Gegensatz zu § 40 Abs. 5 POG – unverändert geblieben.[789] Insofern stellt sich insbesondere die Frage, ob sich auf diese Ausschlussgründe auch der erst später eingefügte Richtervorbehalt des § 40 Abs. 5 POG bezieht. Die Ursprungsfassung des § 40 Abs. 5 POG sah in Satz 2 lediglich vor, dass der Landesdatenschutzbeauftragte zu benachrichtigen ist, sofern die Benachrichtigung auch drei Jahre nach Abschluss der Maßnahme noch nicht erfolgt ist.[790] Nach der damaligen Gesetzeslage ging der Gesetzgeber davon aus, dass das Vorliegen der Ausnahmetatbestände nach Abs. 6 auch die Information des Landesdatenschutzbeauftragten ausschließt.[791] Bei Einfügung des Richtervorbehalts in Abs. 5 hielt der Gesetzgeber fest, dass dieses Instrument die bislang durch den Landesdatenschutzbeauftragten ausgeübte Kontrolle ersetzt.[792] Insofern ist davon auszugehen, dass die Feststellung des Vorliegens eines Ausnahmetatbestandes nach der Rechtslage in Rheinland-Pfalz nicht einem Richter vorbehalten ist; vielmehr sind hier die jeweils zuständigen Ermittlungsbehörden zur Entscheidung berufen.

Bedenken gegen diese Ausgestaltung der Ausnahmetatbestände bestehen unter verfassungsrechtlichen Aspekten grundsätzlich nicht, zumindest nicht, soweit die einzelnen Ausnahmetatbestände verfassungskonform ausgelegt werden. Denn das BVerfG erkennt an, dass bei nur zufällig von einer nicht offenen Datenerhebung Betroffenen die Möglichkeit eines nur unerheblichen Grundrechtseingriffs besteht. Sofern in diesen Fällen davon auszugehen ist, dass die solchermaßen Betroffenen kein Interesse an der Benachrichtigung haben, kann sie unterbleiben.[793] Eine richterliche Bestätigung dieser Abwägungsentscheidung ist nicht notwendig;[794] sie kann beispielsweise der Staatsanwaltschaft überlassen bleiben.[795]

---

789 Die heutige Fassung des § 40 Abs. 6 POG ist bereits in Landesregierung, LT-Drs. 14/2287, S. 23 zu finden.

790 Landesregierung, LT-Drs. 14/2287, S. 23.

791 Landesregierung, LT-Drs. 14/2287, S. 53.

792 Fraktionen der SPD und FDP, LT-Drs. 14/3936, S. 12.

793 BVerfG, Urt. v. 12.10.2011 – 2 BvR 236/08, Rn. 226; BVerfGE 125, 260, 337.

794 BVerfG, Urt. v. 12.10.2011 – 2 BvR 236/08, Rn. 231 f.; BVerfGE 125, 260, 337.

795 BVerfG, Urt. v. 12.10.2011 – 2 BvR 236/08, Rn. 231.

3.3.12.6 § 40 Abs. 6 Nr. 1 POG

Was den Ausschlussgrund des § 40 Abs. 6 Nr. 1 POG anbelangt, ist zu berücksichtigen, dass sich diese Normierung ausdrücklich nur mit der Zielperson der Maßnahme befasst. Die Gesetzesbegründung spricht in diesem Zusammenhang davon, dass der „Betroffene“ zum „Beschuldigten“ wird und somit die strafprozessualen Bestimmungen Anwendung finden.[796] Zur insoweit inhaltsgleichen Regelung in Hamburg hielt das BVerfG fest, dass die Norm auch den Fall betrifft, dass ein Strafverfahren gegen die Zielperson eingeleitet wird, von der Datenerhebung aber auch weitere Personen betroffen waren. In diesen Fällen unterbleibt die Benachrichtigung durch die Polizei.[797] Da eine Benachrichtigung im Rahmen des strafrechtlichen Ermittlungsverfahrens zwingend nur für den Beschuldigten vorgesehen ist (§ 170 Abs. 2 S. 2 StPO), ist die Bestimmung unter dem Aspekt des Grundrechtsschutzes verfassungskonform auszulegen, so dass die Suspendierung der Benachrichtigungspflicht nur gilt, „sofern und solange die Geheimhaltung für die Zwecke der Strafverfolgung erforderlich ist.“[798] Insofern entfällt die Sperre der Benachrichtigung nicht nur, wenn „absehbar ist, dass die sachgerechte Durchführung eines strafrechtlichen Ermittlungsverfahrens durch die Benachrichtigung nicht gefährdet werden kann“, sondern auch „wenn die erhobenen Daten nicht in das Ermittlungsverfahren eingeführt worden sind.“ Daher lebt spätestens nach Abschluss des Ermittlungsverfahrens „die polizeirechtliche Benachrichtigungspflicht wieder auf, sofern das Informationsinteresse der Betroffenen weiter gegeben ist. Hat der Betroffene allerdings schon im Zuge des Ermittlungsverfahrens Kenntnis von der Maßnahme erhalten, besteht kein rechtlich schutzwürdiges Interesse an einer Benachrichtigung mehr.“[799] Das Unterbleiben der Benachrichtigung nur Mit-Betroffener ist nach Auffassung des BVerfG zum einen grundsätzlich an weniger strengen Maßstäben zu messen. Zum anderen dürfte hier die Annahme greifen, dass ein Strafverfahren im Regelfall in absehbarer Zeit entweder vollständig beendet wird oder die Geheimhaltungsinteressen wegfallen, so dass auch nur mit-betroffene Personen bei entsprechendem Interesse in absehbarer Zeit von der Datenerhebung Kenntnis erlan-

---

796 Landesregierung, LT-Drs. 14/2287, S. 53.

797 BVerfG, NVwZ 2001, 1261, 1263.

798 BVerfG, NVwZ 2001, 1261, 1263.

799 BVerfG, NVwZ 2001, 1261, 1263.

gen, weil in diesen Fällen die polizeiliche Benachrichtigungspflicht wieder auflebt – sofern der nur Mit-Betroffene nicht bereits im Rahmen des Strafverfahrens von der Datenerhebung in Kenntnis gesetzt wurde.

3.3.12.7 § 40 Abs. 6 Nr. 2 POG

Nach § 40 Abs. 6 Nr. 2 POG wird endgültig von der Benachrichtigung abgesehen, wenn zur Feststellung der Identität der betroffenen Person weitere Daten erhoben werden müssten und dies im Interesse der Person nicht geboten erscheint. Diese Vorschrift bezieht sich ausweislich der Gesetzesbegründung nicht auf die eigentliche Zielperson der Maßnahme, sondern ausschließlich auf Personen, die von der Datenerhebung nur zufällig betroffen wurden.[800] Liegt lediglich ein nur unerheblicher Grundrechtseingriff vor und es kann unterstellt werden, dass der Betroffene kein Interesse an der Benachrichtigung hat,[801] ist in der verfassungsgerichtlichen Rechtsprechung anerkannt, dass Ausnahmen von der Benachrichtigungspflicht gerechtfertigt sein können, „wenn ihr überwiegende Belange einer betroffenen Person entgegenstehen, etwa weil durch die Benachrichtigung von einer Maßnahme, die keine weiteren Folgen gehabt hat, der Grundrechtseingriff noch vertieft würde.“[802, 803] Bezüglich des – abweichend formulierten – § 101 Abs. 4 S. 5 StPO ging das Bundesverfassungsgericht ausdrücklich davon aus, dass die Entscheidung über das Absehen von der Benachrichtigung der nur Mit-Betroffenen den Ermittlungsbehörden übertragen werden durfte.[804]

---

800 Landesregierung, LT-Drs. 14/2287, S. 53 f. Dies entspricht der Rechtslage nach § 101 Abs. 4 S. 5 StPO, auch wenn diese Vorschrift im Wortlaut deutlich abweicht.

801 BVerfG, Urt. v. 12.10.2011 – 2 BvR 236/08, Rn. 226; BVerfGE 125, 260, 337; ThürVfGH, Urt. v. 21.11.2012 – 19/09, Rn. 275.

802 BVerfG, Urt. v. 12.10.2011 – 2 BvR 236/08, Rn. 227 und 233 ; BVerfGE 125, 260, 336.

803 Es wäre darüber hinaus sogar möglich, den für die Ermittlung der Identität des Betroffenen erforderlichen Aufwand in die Abwägung einzustellen; vgl. BVerfG, Urt. v. 12.10.2011 – 2 BvR 236/08, Rn. 233 und ThürVfGH, Urt. v. 21.11.2012 – 19/09, Rn. 276.

804 BVerfG, Urt. v. 12.10.2011 – 2 BvR 236/08, Rn. 233.

3.3.12.8 § 40 Abs. 6 Nr. 3 POG

Nach § 40 Abs. 6 Nr. 3 POG unterbleibt die Benachrichtigung, wenn keine Aufzeichnungen mit personenbezogenen Daten erstellt oder diese unverzüglich nach Beendigung der Maßnahme vernichtet worden sind. Damit kann in all jenen Fallkonstellationen, in denen z.B. ein bloßes Mithören oder Mitlesen erfolgt ist, ohne dass die Daten gesichert worden wären, oder in denen erhobene Daten sofort nach Ende der Maßnahme vernichtet wurden, ohne vorherige Abwägungsentscheidung auf die Benachrichtigung verzichtet werden. Das BVerfG billigte den Verzicht auf die Benachrichtigung zumindest in den Fällen, in denen „die erfaßten Daten ohne weitere Schritte sogleich als irrelevant vernichtet worden sind.“[805] Unproblematisch ist unter dieser Prämisse die erste Alternative des § 40 Abs. 6 Nr. 3 POG, da hier von vornherein keine Manifestation der erhobenen Daten erfolgt ist. Zweifel könnten aber bezüglich der zweiten Alternative aufkommen, da demnach die Benachrichtigung unterbleiben kann, wenn die erhobenen Daten unverzüglich nach Beendigung der Maßnahme vernichtet werden. Hier stellt sich die Frage, ob die Formulierung der Verfassungsrichter, wonach die Daten „ohne weitere Schritte sogleich als irrelevant“ vernichtet worden sein müssen, den rheinland-pfälzischen Ausnahmetatbestand noch deckt. In Anlehnung an die zur Rasterfahndung entwickelten Grundsätze[806] könnte hier daran zu denken sein, dass die Vernichtung unmittelbar nach der Datenerfassung erfolgen muss und nicht erst nach Ende der gesamten Maßnahme. Hierfür spricht, dass die Vernichtung unmittelbar nach der Datenerhebung nur einen äußerst geringen Eingriff darstellt; bleiben die Daten aber während der gesamten Maßnahme, die sich unter Umständen über einen langen Zeitraum erstrecken kann, verfügbar und damit auch potenziell nutzbar, wiegt der Grundrechtseingriff deutlich schwerer. Daher erscheint es geboten, in diesen Fällen eine Abwägungsentscheidung, wie sie § 40 Abs. 6 Nr. 2 POG richtigerweise vorsieht, zu fordern. Der quasi automatische Benachrichtigungsverzicht nach § 40 Abs. 6 Nr. 3 POG sollte auf eng begrenzte Ausnahmefälle beschränkt bleiben. Dem könnte über eine verfassungskonforme Interpretation der Vorschrift dahingehend Rechnung getragen werden, dass der Begriff der „Maßnahme“ als jeweils konkrete Datenerhebungsmaßnahme verstanden wird und nicht als gesamte Ermittlungsmaßnahme, die sich aus zahlreichen Einzelmaßnahmen zusammensetzen und sich über einen längeren Zeitraum erstrecken kann. Unter den Aspekten der Normenklarheit und -bestimmtheit könnte allerdings auch über eine entsprechende gesetzliche Klarstellung nachgedacht werden.

---

805 BVerfG, Urt. v. 14.07.1999 – 1 BvR 2226/94 u.a., Rn. 294.

4. Empirische Analyse der evaluationsrelevanten POG-Eingriffsnormen

4.1 Zentrale Ergebnisse der Fallzahlenerhebung bei den sechs rheinland-pfälzischen Polizeibehörden

Wie bereits im Kapitel 2 beschrieben wurde, kamen bei der empirischen Analyse der Anwendungspraxis der gemäß § 100 POG zu evaluierenden Normen mit den Erhebungsbögen zur Fallzahlenanalyse sowie den leitfadengestützten Interviews zwei unterschiedliche Erhebungsinstrumente zum Einsatz. In den folgenden Abschnitten werden die zentralen Ergebnisse der quantitativen Erfassung der Anwendungsfälle, die während des Evaluationszeitraums von den sechs rheinland-pfälzischen Polizeibehörden erhoben wurden, vorgestellt.

4.1.1 Allgemeine Struktur des Rücklaufs

Im Evaluationszeitraum (15.02.2011 bis 31.03.2016) sind von den sechs rheinland-pfälzischen Polizeibehörden insgesamt zu 36 abgeschlossenen Maßnahmen Erhebungsbögen übermittelt worden. 35 Maßnahmen betrafen die Datenerhebung durch den Einsatz technischer Mittel zur Überwachung und Aufzeichnung der Telekommunikation, Auskunft über Telekommunikation gemäß § 31 Abs. 1 POG. Neben den abgeschlossenen Maßnahmen hat das Polizeipräsidium Mainz im Evaluationszeitraum auch fünf Erhebungsbögen zu Maßnahmen nach § 31 Abs. 1 POG übermittelt, die nicht abgeschlossen wurden. In zwei Fällen handelte es sich um je eine Vermisstensache. Es wurde jeweils ein Antrag zur Durchführung der Datenerhebungsmaßnahme beim OVG Koblenz gestellt. Bevor die beiden Anträge beschieden wurden, tauchten die vermissten Personen jedoch wieder auf, so dass keine Datenerhebung gemäß § 31 Abs. 1 POG erfolgte. Bei der dritten Maßnahme, die nicht abgeschlossen wurde, handelte es sich um einen Fall, in dem eine Person mit dem Einsatz einer Schusswaffe gedroht hatte. Auch hier wurde eine Datenerhebung ge-

806 Vgl. hierzu die Ausführungen unter Ziff. 3.3.8.1. Sofern Daten nur „ungezielt und allein technikbedingt zunächst miterfasst, aber unmittelbar nach der Erfassung technisch wieder anonym, spurenlos und ohne Erkenntnisinteresse für die Behörden ausgesondert werden“, liegt schon kein Grundrechtseingriff vor, BVerfG, Urt. v. 04.04.2006 – 1 BvR 518/02, Rn. 74.

mäß § 31 Abs. 1 POG beantragt, jedoch vom OVG abgelehnt. Stattdessen erfolgte lediglich eine Handyortung gemäß § 31a POG. In zwei weiteren Fällen (Bedrohung und zu erwartende Gebietsstreitigen/gewalttätige Ausschreitungen im Rockermilieu zwischen zwei Gruppierungen) wurde der Antrag auf Durchführung einer Maßnahme gemäß § 31 Abs. POG ebenfalls vom OVG abgelehnt. Das Gericht begründet seine Entscheidung damit, dass es an einer konkreten und gegenwärtigen Gefahr für ein von § 31 Abs. 1 POG geschütztes Rechtsgut fehle. Des Weiteren wurde vom Polizeipräsidium Rheinpfalz eine Maßnahme gemäß § 31 Abs. 1 POG beim OVG beantragt, über den das Gericht auch positiv entschieden hat. Da allerdings nach dem Stand der Ermittlungen auch von einem Gewaltverbrechen ausgegangen werden konnte, erging zudem ein Beschluss gemäß § 100a StPO vom zuständigen Amtsgericht, auf dessen Grundlage die Maßnahme dann durchgeführt wurde. Somit erfolgte keine Datenerhebung gemäß § 31 Abs. 1 POG.

Auffällig ist, dass auf die Polizeipräsidien Mainz (18) und Koblenz (9) drei Viertel der im Evaluationszeitraum durchgeführten Maßnahmen gemäß § 31 Abs. 1 POG entfallen. Die verbleibenden acht Maßnahmen verteilen sich auf die Polizeipräsidien Rheinpfalz (5), Trier und Westpfalz sowie das LKA (je 1). Hinsichtlich der Entwicklung der Fallzahlen lässt sich keine eindeutige Tendenz feststellen. Insbesondere lässt sich nicht erkennen, dass die Polizeibehörden verstärkt die z.T. neuen Möglichkeiten zur verdeckten Datenerhebung nutzen. Anhand von Tab. 2 wird deutlich, dass – bezogen auf den gesamten Erhebungszeitraum – durchschnittlich eine verdeckte Datenerhebungsmaßnahme pro Polizeibehörde und Jahr in Rheinland-Pfalz durchgeführt wurde.

Im Gegensatz zum ersten Erhebungszeitraum ist im zweiten Erhebungszeitraum erstmalig auch vom Polizeipräsidium Mainz eine Maßnahme gemäß § 31b POG (Auskunft über Nutzungsdaten) durchgeführt worden.

Die übrigen Datenerhebungsmaßnahmen sind im Evaluationszeitraum dagegen nicht zur Anwendung gekommen. Somit konzentriert sich die nachfolgende Auswertung auf die nach § 31 Abs. 1 POG durchgeführten Maßnahmen zur Überwachung und Aufzeichnung der Telekommunikation.

Tab. 2: Anzahl der durchgeführten Maßnahmen gemäß § 31 Abs. 1 POG nach Polizeibehörden und Erhebungszeiträumen

PP/ Zeitraum	PP Koblenz	PP Mainz	PP Rhein-pfalz	PP Trier	PP West-pfalz	LKA	Ge-samt
15.02.2011-31.07.2012	4	6	2	0	0	0	**12**
01.08.-30.11.2012	1	1	0	0	0	0	**2**
01.12.2012-31.03.2013	1	0	0	0	0	0	**1**
01.04.-30.09.2013	3	7	0	0	0	0	**10**
01.10.2013-31.03.2015	0	2	3	1	0	1	**7**
01.04.-30.09.2015	0	0	0	0	0	0	**0**
01.10.2015-31.03.2016	0	2	0	0	1	0	**3**
Gesamt	**9**	**18**	**5**	**1**	**1**	**1**	**35**

4.1.2 Anlass für die Datenerhebung und polizeiliche Vorgehensweise

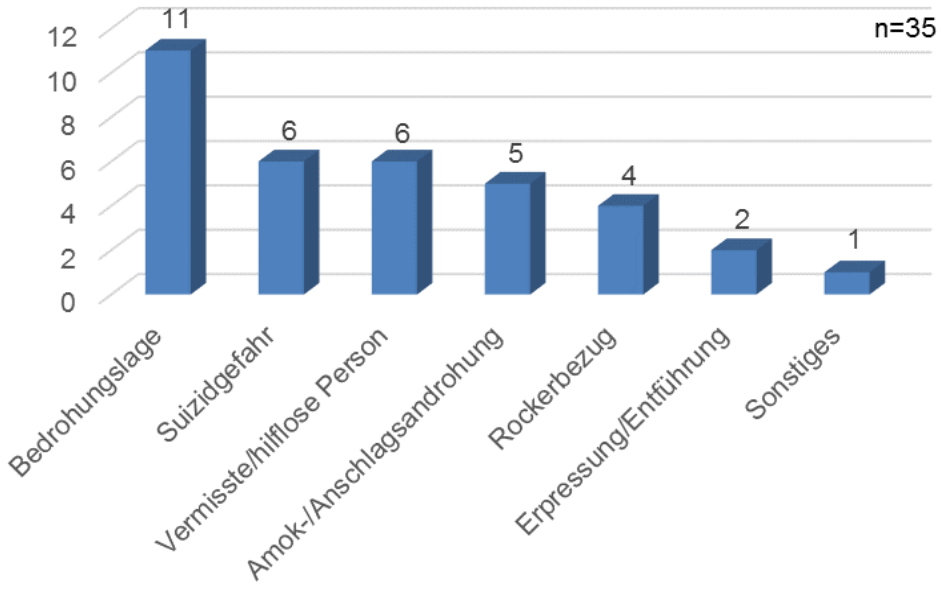
Im Rahmen der fallbezogenen Erhebung bei den rheinland-pfälzischen Polizeibehörden ging es zunächst darum herauszufinden, aus welchem Anlass Daten durch den Einsatz technischer Mittel zur Überwachung und Aufzeichnung der Telekommunikation erhoben worden sind. Bei 32 Maßnahmen gemäß § 31 Abs. 1 POG ist ausschließlich angegeben worden, dass die Datenerhebung durchgeführt worden ist, um eine gegenwärtige Gefahr für Leib oder Leben einer Person abzuwehren. In zwei weiteren Fällen ging es zusätzlich darum, eine gegenwärtige Gefahr für Güter der Allgemeinheit (Bedrohung der Grundlage oder des Bestands des Staates oder Grundlagen der Existenz der Menschen) abzuwehren. In einem Fall war dies der alleinige Grund für die Durchführung der Datenerhebungsmaßnahme.

Darüber hinaus haben die Polizeibehörden bei jeder durchgeführten Maßnahme zusätzlich angegeben, um was für eine Gefahrenlage es sich in dem jeweiligen Fall gehandelt hat. In elf Fällen lag eine allgemeine Bedrohungslage

vor, die nicht näher beschrieben wurde. In sechs Fällen wurden Datenerhebungsmaßnahmen gemäß § 31 Abs. 1 POG durchgeführt, da die Gefahr eines Suizidversuchs bestand. In sechs weiteren Fällen dienten die Maßnahmen dazu, vermisste bzw. hilflose Personen aufzuspüren. Bei fünf Fällen bestand die Gefahrenlage darin, dass es Hinweise auf eine Amoktat bzw. einen Anschlag gab.

In vier Fällen ging es um die Abwehr von Gefahren, die im Zusammenhang mit Rockern standen. In je zwei Fällen lagen Hinweise für eine Erpressung/Entführung vor. In einem Fall, der keiner der anderen Kategorien zugeordnet werden konnte, handelte es sich um eine Auseinandersetzung in der Fußballszene. Anhand dieser Ergebnisse zeigt sich, dass die Datenerhebungsmaßnahme gemäß § 31 Abs. 1 POG in verschiedenen Bereichen zur Anwendung kam. Eine eindeutige Schwerpunktbildung lässt sich allerdings nicht erkennen, auch wenn in knapp einem Drittel der Fälle die rechtlichen Möglichkeiten dazu genutzt wurden, um suizidgefährdete Personen im speziellen und vermisste/hilflose Personen im Allgemeinen aufzuspüren.

Abb. 1: Gefahrenlagen im Zusammenhang mit den Maßnahmen nach § 31 Abs. 1 POG



Hinsichtlich der polizeilichen Vorgehensweise zur Feststellung einer gegenwärtigen Gefahr im Sinne von § 31 POG vor Durchführung einer Datenerhebung durch den Einsatz technischer Mittel zur Überwachung und Aufzeichnung der Telekommunikation, Auskunft über Telekommunikation fällt auf, dass in zehn Fällen keine geeigneten Maßnahmen vorhanden gewesen sind.

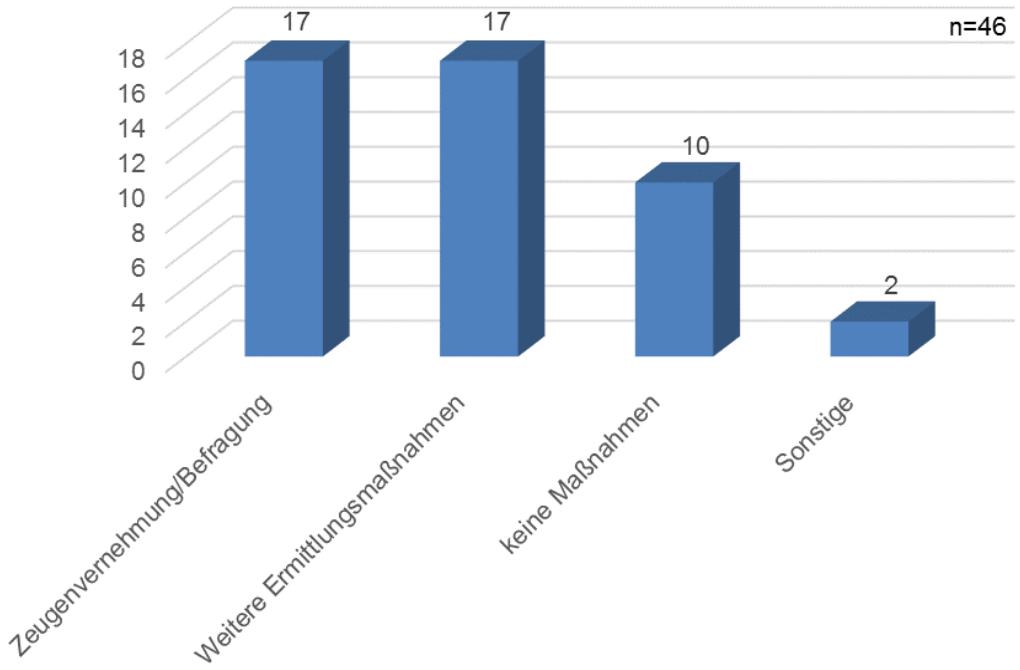
In 17 Fällen wurden Zeugenvernehmungen/Befragungen entweder ausschließlich (acht Fälle) oder in Verbindung mit weiteren Maßnahmen (neun Fälle) durchgeführt, um eine gegenwärtige Gefahr im Sinne von § 31 POG festzustellen. In zwei Fällen gab es neben Befragungen noch weitere Ermittlungen im persönlichen Umfeld der vermissten Person. In einem Fall wurde zusätzlich zur Befragung des Ehemanns noch Einsicht in die übermittelten SMS genommen. In einem anderen Fall wurde ergänzend zur Angehörigen- und Nachbarschaftsbefragung noch eine Wohnungsdurchsuchung durchgeführt. Bei einem Fall gab es zusätzlich zu den Zeugenaussagen noch weitere Aufklärungsmaßnahmen sowie einen Informationsaustausch zwischen den Fachdienststellen. In einem Fall wurde neben der Zeugenvernehmung und der Nachbarschaftsbefragung noch eine Personen- und Fahrzeugfahndung eingeleitet. Bei einem Fall wurden zusätzlich zur Zeugenbefragung weitere Maßnahmen genannt (z.B. Abklärung Arbeitsstelle). In einem anderen Fall wurde ergänzend zur Befragung der Mitarbeiterin, die das Gespräch entgegen genommen hatte, das Protokoll der Mitarbeiterin sichergestellt. In einem Fall erfolgten zur Feststellung des Vorliegens einer gegenwärtigen Gefahr zusätzlich zur Befragung eine Auswertung der Notrufaufzeichnungen/Rettungsleitstelle, eine Hausdurchsuchung beim Ehemann sowie eine Durchsuchung der Gefährderin.

In acht Fällen wurden ausschließlich andere Ermittlungsmaßnahmen seitens der Polizei zur Feststellung einer gegenwärtigen Gefahr ergriffen. In zwei Fällen führte die zuständige Polizeibehörde (einmal beim Jugendamt) Ermittlungen durch. In zwei weiteren Fällen wurde mit Hilfe der Telefonanlage versucht weiterführende Erkenntnisse zu sammeln (ein Rückrufversuch und ein Abruf von Anrufzeiten, Rufnummern etc.). Bei einem Bedrohungsfall wurde eine Handyortung gemäß § 31a POG vorgeschaltet. In einem weiteren Fall erfolgte eine Tatbestandsaufnahme (Bedrohung mit Schusswaffe sowie Suizidandrohung).

In einem Fall wurde eine Nahbereichsfahndung im Zusammenhang zusammen mit einer Standortfeststellung nach § 31a POG durchgeführt.

Darüber hinaus setzte die Polizei in einem Fall zur Feststellung des Vorliegens einer gegenwärtigen Gefahr auf besondere Mitte der verdeckten Datenerhebung (§ 28 POG) sowie auf polizeiliche Beobachtung (§ 32 POG).

Abb. 2: Maßnahmen zur Feststellung der gegenwärtigen Gefahr im Sinne von § 31 POG[807]



Darüber hinaus sind die Polizeibehörden dazu befragt worden, welche Datenerhebungsmaßnahmen als milderes Mittel zur Vermeidung von Maßnahmen nach § 31 POG ergriffen worden sind. In knapp der Hälfte der Fälle (17) gab es keine andere Möglichkeit, die benötigten Daten zu erhalten als mit Maßnahmen nach § 31 POG. In 18 Fällen griffen die Polizeibehörden zunächst auf andere Maßnahmen zur Datenerhebung zurück. In sechs Fällen wurden seitens der Polizei Befragungen (z.B. Zeugen, Nachbarschaft, Angehörige) als milderes Mittel durchgeführt, wobei in vier Fällen weitere Maßnahmen genutzt wurden, um die erforderlichen Informationen zu erhalten (Wohnungsdurchsuchung, Fahndung, Abklärung Arbeitsstelle, InPOL-Ausschreibungen, Handyortung, Überprüfungen bei der Bundespolizei am Flughafen Frankfurt, Überprüfung diverser Anlaufadressen, Einsatz eines Personenspürhundes).

In drei Fällen suchte die Polizei die jeweilige Kontaktadresse auf, wobei in zwei Fällen zusätzlich eine Nahbereichsfahndung eingeleitet bzw. in einem Fall auch noch der Versuch unternommen wurde, sich mit dem Suizidenten zu verabreden. In vier Fällen nutzte die Polizei soziale Netzwerke zur Datenerhebung, wobei hier in jeweils zwei Fällen zusätzlich noch eine Ortung des Handys

807 Das hier angegebene n ist größer als 35, da pro Fall z.T. mehr als eine Maßnahme zur Feststellung der gegenwärtigen Gefahr gemäß § 31 POG genutzt wurde.

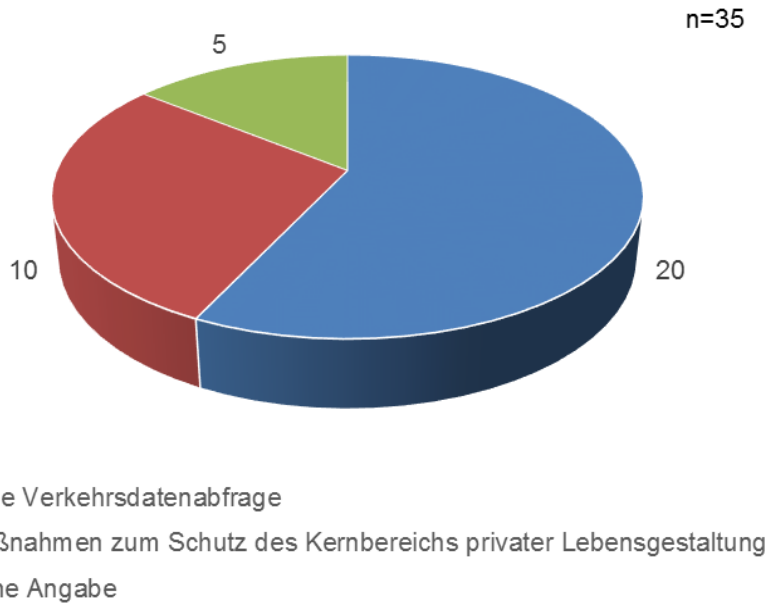
gemäß § 31a POG und eine Durchsuchung der Wohnung sowie eine Veröffentlichung in der Presse erfolgte. In drei Fällen griffen die Polizeibehörden zunächst auf die Möglichkeit gemäß § 31a POG zurück, wobei in einem Fall zusätzlich eine Wohnung durchsucht und in einem anderen Falls eine Nahbereichsfahndung eingeleitet wurde.

In einem Fall wurde die Observation als milderes Mittel zur Vermeidung von Maßnahmen nach § 31 POG genutzt. In einem Fall wurde zunächst eine Nahbereichsfahndung eingeleitet sowie eine Standortfeststellung gemäß § 31a POG durchgeführt, um weiterführende Erkenntnisse zu gewinnen. In einem anderen Fall wurde zunächst versucht, über die zentrale Telefonanlage Auskünfte über Anrufzeiten, Rufnummern etc. zu erhalten.

Die Ergebnisse zeigen, dass die Polizeibehörden zunächst versuchen, alle ihnen zur Verfügung stehenden Maßnahmen zur Informationsgewinnung zu nutzen, bevor eine verdeckte Datenerhebung durchgeführt wird, wenngleich es auch einige Fälle gab, in denen offenbar keine geeigneten milderen Maßnahmen zur Verfügung standen.

Im Zusammenhang mit der Durchführung von Datenerhebungsmaßnahmen gemäß § 31 Abs. 1 POG wurden die Polizeibehörden zudem danach gefragt, welche Vorkehrungen getroffen wurden, um den Schutz des Kernbereichs privater Lebensgestaltung sicherzustellen. Beim überwiegenden Teil der Fälle (20) waren solche Vorkehrungen aus Sicht der Polizeibehörden nicht erforderlich, da im Zuge der Maßnahme lediglich Verkehrsdaten erhoben wurden und somit der Kernbereich nicht betroffen war. Hingegen wurden in zehn Fällen Vorkehrungen zum Kernbereichsschutz getroffen. Hierzu zählten die Begrenzung der durch die Maßnahme betroffenen Personen auf die Führungskader der Konfliktparteien, die Kennzeichnung der Kernbereichsgespräche und Löschung nach Weisung des OVG, keine Berührung des Kernbereichs (ansonsten vorübergehende Abschaltung), Nutzung einer Auswertungssoftware und damit einhergehend namentliche Zuweisung von Rufnummern, selektives Hineinhören in erkennbare Gespräche ohne Rockerbezug, Einbindung des Datenschutzbeauftragten bzw. Bestellung eines Kernbereichsbeauftragten, unmittelbare Abschaltung der Maßnahme nach Lokalisierung des Anschlussinhabers sowie Überprüfung der Kommunikationsinhalte durch den Leiter der Abteilung 1 und den Datenschutzbeauftragten des LKA. In fünf Fällen hat die Polizeibehörde keine Angaben zu Vorkehrungen zum Kernbereichsschutz gemacht.

Abb. 3: Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung



Somit wird deutlich, dass in vielen Fällen die Maßnahmen so angelegt sind, dass sie erst gar nicht den Kernbereich der privaten Lebensgestaltung berühren. Im weit überwiegenden Teil der Fälle, in denen dies nicht vermeidbar ist, treffen die Polizeibehörden Vorkehrungen, um den Schutz des Kernbereichs zu gewährleisten.

4.1.3 Von der Datenerhebung betroffene Personen

Im Rahmen der Evaluation wurden die Polizeibehörden dazu befragt, gegen wie viele Personen sich die Maßnahme gemäß § 31 Abs. 1 POG nach dem Beschluss bzw. nach der Anordnung gerichtet hat. Insgesamt richteten sich die durchgeführten Datenerhebungsmaßnahmen nach Beschluss bzw. nach Anordnung gegen 347 Personen, was etwa 10 Personen pro Fall entspricht. Jedoch verzerrt diese Darstellung das tatsächliche Bild, da in 22 Fällen eine verdeckte Datenerhebung lediglich gegen eine Person angeordnet wurde, während in acht Fällen die Maßnahme gemäß § 31 Abs. 1 POG gegen zwei Personen angeordnet wurde. In je einem Fall richtet sich die Maßnahme nach Anordnung bzw. Beschluss gegen drei, vier bzw. sieben Personen. Bei zwei Fällen handelt es sich um deutliche Sonderfälle, da sich die Datenerhebung in dem ersten Fall gegen 175 Personen und in dem zweiten Fall gegen 120 Personen richtete und sie damit deutlich über dem Durchschnitt knapp zehn Personen

liegt. Ohne diese beiden Extremfälle liegt der Durchschnitt hingegen bei 1,6 Personen pro Maßnahme.

Adressaten einer Maßnahme gemäß § 31 POG können die Verantwortlichen für eine Gefahr (Verhaltensstörer gemäß § 4 POG bzw. Zustandsstörer gemäß § 5 POG), nicht verantwortliche Dritte gemäß § 7 POG sowie Nachrichtenmittler (§ 31 Abs. 1 S. 1 Nr. 2 POG) sein.[808]. Tab. 3 gibt einen Überblick darüber, gegen welche und wie viele Adressaten sich die Maßnahmen gerichtet haben. Insgesamt wurde im Evaluationszeitraum eine Datenerhebung gegen 30 Verhaltensstörer, 312 nicht verantwortliche Dritte sowie fünf Nachrichtenmittler angeordnet. Gegen Zustandsstörer gemäß § 5 POG wurde bislang hingegen keine Maßnahme angeordnet. Auffällig ist, dass sich gewisse Unterschiede zwischen den zuständigen Polizeibehörden ergeben. Während sich die Anordnungen zur Datenerhebung bei den beiden Polizeipräsidien Koblenz und Rheinpfalz durchschnittlich gegen eine bzw. zwei Person(en) richteten, sind es beim Polizeipräsidium Mainz 18 Personen pro Maßnahme. Jedoch ist bei dem Ergebnis des Polizeipräsidiums Mainz darauf hinzuweisen, dass dies auf zwei Anordnungen zurückzuführen ist, die sich gegen eine sehr hohe Anzahl nicht verantwortlicher Dritter richtete. Dabei ging es um die Erhebung von Verkehrsdaten im Zusammenhang mit der telefonischen Ankündigung eines schweren sexuellen Missbrauchs von einem Kind bei der Telefonseelsorge und sowie im Zusammenhang mit einer Amokandrohung. Ohne diese beiden Extremfälle liegt der Durchschnitt beim Polizeipräsidium Mainz ebenfalls nur bei einer Person pro Maßnahme.

Tab. 3: Anordnung der verdeckten Datenerhebung gemäß § 31 Abs. 1 POG nach Personengruppen und Polizeibehörden

Polizeibehörde	Verhaltensstörer	Zustandsstörer	Nicht verantwortliche Dritte	Nachrichtenmittler	Gesamt
PP Koblenz	8	0	5	2	15
PP Mainz	17	0	300	1	318
PP Rheinpfalz	2	0	3	0	5
PP Trier	1	0	0	0	1
PP Westpfalz	1	0	4	2	7
LKA	1	0	0	0	1
Gesamt	**30**	**0**	**312**	**5**	**347**

808 *Roos/ Lenz*, POG, § 31, Rn. 5; Landesregierung, LT-Drs. 15/4879, S. 31

Betrachtet man fallbezogen, gegen wenn sich die Anordnungen gerichtet haben, ergibt sich folgendes Bild: In 27 Fällen wurde die Datenerhebung gemäß § 31 Abs. 1 POG über insgesamt 30 Verhaltensstörer angeordnet, wobei sich diese in sieben Fällen auch gegen nicht verantwortliche Dritte richtete (dreimal eine Person sowie je einmal zwei Personen, drei Personen, 119 Personen und 174 Personen). Zudem richtete sich eine Maßnahme zusätzlich noch gegen einen Nachrichtenmittler. In einem anderen Fall wurde die Maßnahme gegen einen Verhaltensstörer, vier nicht verantwortliche Dritte sowie zwei Nachrichtenmittler angeordnet.

In sieben Fällen sollten ausschließlich über je einen nicht verantwortlichen Dritten Daten verdeckt erhoben werden, während sich in einem Fall die Datenerhebungsmaßnahme gemäß § 31 Abs. 1 POG ausschließlich gegen zwei Nachrichtenmittler richtete. In keinem Fall wurde eine Datenerhebung über Zustandsstörer angeordnet. Daran wird deutlich, dass sich die Anordnung der Maßnahme gemäß § 31 Abs. 1 POG hauptsächlich gegen Verhaltensstörer richtet, während nicht verantwortliche Dritte und Nachrichtenmittler eine untergeordnete Rolle spielen und seltener bzw. deutlich seltener von einer Anordnung betroffen sind. Ebenfalls erkennbar ist, dass sich die Anordnungen im Regelfall gegen eine oder zwei Person(en) richten.

Entscheidend für die Bewertung der Eingriffsintensität der Maßnahmen ist jedoch nicht nur die Anzahl der in der Anordnung genannten Personen, sondern auch die Anzahl der Personen, die tatsächlich von der Datenerhebung betroffen worden sind. Aus diesem Grund wurden die Polizeibehörden danach gefragt, über wie viele Personen im Zuge der Maßnahme gemäß § 31 Abs. 1 POG tatsächlich Daten erhoben wurden. Nach Angaben der sechs Polizeibehörden wurden im Evaluationszeitraum über 441 Personen Daten erhoben, wobei 386 Personen davon als Dritte eingestuft wurden. Im Durchschnitt wurden somit über 13 Personen pro Maßnahme Daten erhoben. Betrachtet man die hier übermittelten Fälle genauer, zeigt sich, dass in 26 Fällen nicht über mehr Personen Daten erhoben wurden, als in der Anordnung bzw. im Beschluss genannt wurden. Bei fünf vom Polizeipräsidium Mainz durchgeführten Maßnahmen gemäß § 31 Abs. 1 POG wurden Daten über 71 Personen erhoben, die nicht im Beschluss bzw. in der Anordnung aufgeführt waren. In zwei Fällen stellte sich im Rahmen der Datenerhebung heraus, dass der Verhaltensstörer, gegen den sich die Anordnung bzw. der Beschluss zunächst richtete, doch ein unbeteiligter Dritter war. Bei drei vom PP Rheinpfalz durchgeführten Maßnahmen wurde jeweils über eine Person mehr Daten erhoben, als in der Anordnung angegeben war. In einem anderen Fall wurden zu 19 Personen Daten erhoben, die nicht in der Anordnung genannt waren.

Daran wird deutlich, dass beim Großteil der durchgeführten Maßnahmen nicht über mehr Personen Daten erhoben wurden, als vorher von den Polizeibehörden beantragt worden war. Diese Tatsache deutet auf einen maßvollen Umgang mit der Maßnahme gemäß § 31 Abs. 1 POG seitens der Polizeibehörden hin.

Tab. 4: Anzahl der gemäß Anordnung und tatsächlich betroffenen Personen nach Polizeibehörden

Polizeibehörde	Anzahl der Personen gemäß Anordnung	Anzahl der tatsächlich betroffenen Personen	
		Gesamt	*davon Dritte*
PP Koblenz	15	15	5
PP Mainz	318	389	368
PP Rheinpfalz	5	10	4
PP Trier	1	1	0
PP Westpfalz	7	6	0
LKA	1	20	19
Gesamt	347	441	396

4.1.4 Art der erhobenen Daten

Ebenfalls bei der Bewertung der Eingriffsintensität der Maßnahmen zu berücksichtigen ist die Art der erhobenen Daten. Gemäß § 31 Abs. 2 POG kann sich die Datenerhebung sowohl auf Telekommunikationsinhalte als auch auf Verkehrsdaten erstrecken, wobei bei Letzteren die Erhebung der Daten sowohl laufend als auch retrograd erfolgen kann. Aus diesem Grund wurden die rheinland-pfälzischen Polizeibehörden danach gefragt, welche Daten über die jeweiligen Personen im Evaluationszeitraum erhoben worden sind. Bei der Gesamtauswertung zeigt sich, dass der Schwerpunkt der Datenerhebung gemäß § 31 Abs. 1 POG auf der Erhebung von Verkehrsdaten (56 Mal) liegt, während die Erfassung von Gesprächsinhalten (30 Mal) seltener vorkam. Bezogen auf die 35 übermittelten Fälle bedeutet dies, dass bei 33 Maßnahmen Verkehrsdaten über mindestens eine der o.g. Personengruppen erhoben wurden, während in 12 Fällen von mindestens einer der o.g. Personengruppen zusätzlich

Gesprächsinhalte überwacht wurden. Bei zwei Maßnahmen wurden ausschließlich Gesprächsinhalte überwacht. Somit ist festzuhalten, dass eine ausschließliche Erhebung von Gesprächsinhalten im Rahmen der gemäß § 31 Abs. 1 POG durchgeführten Datenerhebungsmaßnahmen nur in Einzelfällen erfolgte.

Betrachtet man die Verteilung der erhobenen Daten differenziert nach den im Gesetz genannten Personengruppen, ist zunächst festzuhalten, dass in 29 Fällen eine Datenerhebung über Verhaltensstörer (§ 4 POG) erfolgte. In 17 Fällen wurden ausschließlich Verkehrsdaten erhoben, während in zehn Fällen sowohl Verkehrsdaten als auch Gesprächsinhalte erfasst wurden. In zwei Fällen erfolgte eine ausschließliche Erhebung von Gesprächsinhalten der Verhaltensstörer.

Darüber hinaus wurden in 16 Fällen Daten über nicht verantwortliche Dritte (§ 7 POG) erhoben, wobei in zehn Fällen ausschließlich Verkehrsdaten und in fünf Fällen zusätzlich Gesprächsinhalte überwacht worden sind. In einem Fall erfolgte eine ausschließliche Erfassung der Gesprächsinhalte.

In zwei Fällen wurden über Nachrichtenmittler sowohl Verkehrsdaten als auch Gesprächsinhalte erhoben.

In fünf Fällen wurden zudem Daten über unbeteiligte Dritten erhoben, wobei in drei Fällen sowohl Gesprächsinhalte als auch Verkehrsdaten erfasst wurden. In je einem Fall wurden ausschließlich Verkehrsdaten bzw. Gesprächsinhalte erhoben.

Da es gemäß § 31 Abs. 2 POG auch möglich ist, Verkehrsdaten zu erheben, die sich auf Zeiträume vor der Anordnung der Erhebungsmaßnahme erstrecken, wurden die Polizeibehörden auch danach gefragt, in welchen Fällen über welche Personen eine retrograde Erhebung erfolgte. Bei der Gesamtauswertung zeigt sich, dass – ausgehend von den 56 Mal, in denen Verkehrsdaten erhoben wurden – 21 Mal von dieser Möglichkeit Gebrauch gemacht wurde. Insgesamt wurden bei 12 der 35 durchgeführten Maßnahmen gemäß § 31 Abs. 1 POG Verkehrsdaten retrograd erhoben. Hingegen wurde bei 23 Maßnahmen auf eine solche Erhebung verzichtet.

Neben Informationen zur Anzahl und Art der betroffenen Personen wurden bei den Polizeibehörden zudem Informationen zum Umfang der jeweiligen Datenerhebungsmaßnahme abgefragt. Insgesamt wurden im Evaluationszeitraum 66 Telefonanschlüsse (Mobilfunk und Festnetz) überwacht. Bei einer Maßnahme wurde angegeben, dass kein Anschluss überwacht wurde. Im Zuge der durchgeführten Datenerhebungsmaßnahmen gemäß § 31 Abs. 1 POG wa-

ren insgesamt 2.306 Telekommunikationsverbindungen betroffen, wobei jedoch bei 16 Maßnahmen aus unterschiedlichen Gründen keine Angabe zur Zahl der überwachten Telekommunikationsverbindungen gemacht werden konnte. Zu zwei Maßnahmen wurde lediglich angegeben, dass die Zahl der Telekommunikationsverbindungen nicht bekannt ist. Bei zwei weiteren Maßnahmen gab die zuständige Polizeibehörde an, dass hierüber keine Auskunft mehr erteilt werden kann, da die Daten bereits gelöscht wurden. In einem anderen Fall konnte die Polizeibehörde keine Angaben machen, da vom Telefonprovider ein fehlerhafter Datensatz zur Verfügung gestellt worden war. Bei einer Datenerhebungsmaßnahme gab die zuständige Polizeibehörde an, dass keine Kommunikation im Überwachungszeitraum stattgefunden hat. Die Ergebnisse zeigen, dass die Polizeibehörden die Maßnahmen gemäß § 31 Abs. 1 POG hauptsächlich zur Erhebung von Verkehrsdaten nutzen und damit auf die weniger eingriffsintensive Maßnahme zurückgreifen. Sofern dies erforderlich ist, werden nur bzw. zusätzlich Telekommunikationsinhalte sowie retrograde Verkehrsdaten mit erfasst.

4.1.5 Probleme im Zusammenhang mit der Durchführung der Maßnahme

Ziel des Evaluationsvorhabens war es neben der Bewertung der Effektivität und Eingriffsintensität der Datenerhebungsmaßnahmen auch, mögliche Anwendungsprobleme zu erfassen, die den Erfolg der jeweiligen Maßnahme beeinträchtigt haben. Bezogen auf die 35 gemäß § 31 Abs. 1 POG durchgeführten Maßnahmen zeigt sich hier ein eindeutiges Bild. Lediglich in zwei Fällen ist es bei zwei Polizeibehörden zu solchen Problemen gekommen. In dem einen Fall wurde darauf verwiesen, dass das technische Equipment allgemein noch nicht vorhanden ist. In dem anderen Fall ergab sich ein Problem dadurch, dass die Entscheidung des OVG Koblenz durch die Osterfeiertage postalisch verzögert zugestellt wurde. Da die Frist für die Einreichung der Entscheidung im Original bereits überschritten war, hatte der zuständige Provider zwischenzeitlich die Übermittlung abgeschaltet. Nach Einreichung des Originals wurden die Daten wieder übermittelt. Die Telekommunikation, die zwischen der Abschaltung und der zweiten Aktivierung (16 Stunden) stattgefunden hatte, wurde jedoch nicht nachgereicht.

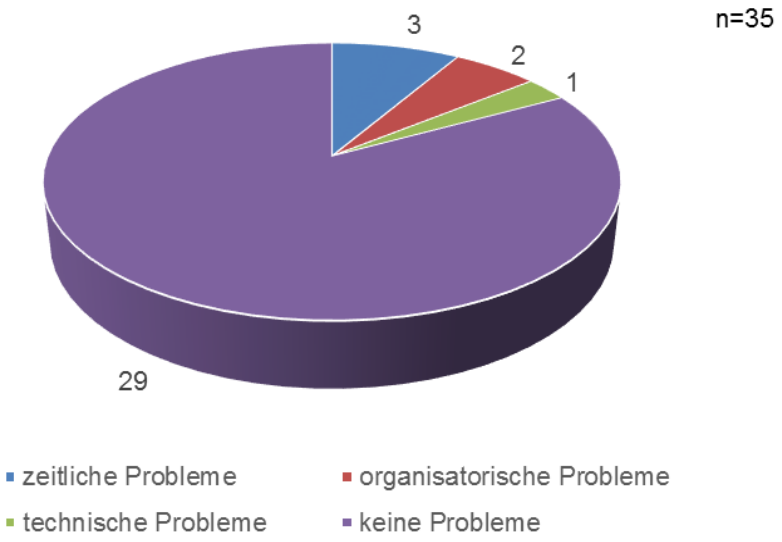
Ebenfalls untersucht werden sollte, ob es Probleme im Zusammenhang mit der Ermöglichung der gewünschten Überwachung oder mit der Erteilung von Auskünften über Verkehrsdaten durch den/die Telekommunikationsdienstleister gab. Hier wurde in sechs Fällen von vier Polizeibehörden auf Probleme hingewiesen. In drei Fällen wurden zeitliche Probleme genannt. So wurde

zweimal eine noch frühzeitigere Übermittlung der Daten durch den Provider gefordert. Im dritten Fall wurde moniert, dass sich die Aufschaltung zeitlich verzögert hatte, da den Providern ein Zeitfenster von bis zu sechs Stunden zur Verfügung steht, um die Maßnahme tatsächlich aufzuschalten.

In zwei Fällen wurden organisatorische Aspekte beim Provider bemängelt. Zum einen wurde seitens der Polizeibehörde kritisiert, dass die Rufbereitschaft des betroffenen Providers mit der gewünschten Datenausleitung überfordert war, da er nicht darauf vorbereitet war, auf Anfragen aus gefahrenabwehrenden Sofortlagen zu reagieren. Zum anderen wurde von einer Polizeibehörde die fehlende Rufbereitschaft bei einem Provider für die Bereitstellung retrograder Verkehrsdaten am Wochenende bemängelt.

In einem Fall ist es zu einem Schaltungsfehler bei einem Provider gekommen.

Abb. 4: Probleme im Zusammenhang mit der Durchführung der Datenerhebungsmaßnahme gemäß § 31 Abs. 1 POG



Ein dritter Aspekt, der im Rahmen der Evaluation berücksichtigt wurde, war, ob es Probleme bei der Einholung der richterlichen Entscheidung gegeben hat. Bei fünf der übermittelten Datenerhebungsmaßnahmen wurde von den Polizeibehörden auf Probleme hingewiesen. In zwei Fällen war der Richter am OVG nicht erreichbar. In einem Fall musste die Maßnahme – trotz Erreichbarkeit des OVG – wegen Gefahr in Verzug durch den Beauftragten des höheren Dienstes angeordnet werden, da das Gericht keine zeitnahe Entscheidung treffen konnte. Das OVG hatte jedoch telefonisch mitgeteilt, dass die Voraussetzungen für die Durchführung der Maßnahme vorliegen. Bei einer anderen Maßnahme handelte es sich dagegen eher um ein internes Problem bei der

Einholung der richterlichen Entscheidung. Insgesamt gibt es im zuständigen Polizeipräsidium nur zwei Volljuristen, die einen Beschluss für eine Maßnahme gemäß § 31 POG beim OVG beantragen können. Allerdings ist dieser Personenkreis außerhalb der Regeldienstzeiten nicht erreichbar, so dass in diesen Zeiten keine Maßnahmen beantragt werden können. In einem fünften Fall gab die Polizeibehörde an, dass das OVG die Anordnung der Maßnahme zunächst abgelehnt hatte.

Dies deutet darauf hin, dass die Zusammenarbeit zwischen dem OVG Koblenz und den beantragenden Polizeibehörden bislang gut funktioniert hat. Aber auch insgesamt bleibt festzuhalten, dass beim Großteil der im Evaluationszeitraum durchgeführten Datenerhebungsmaßnahmen (25)[809] keinerlei Probleme aufgetreten sind.

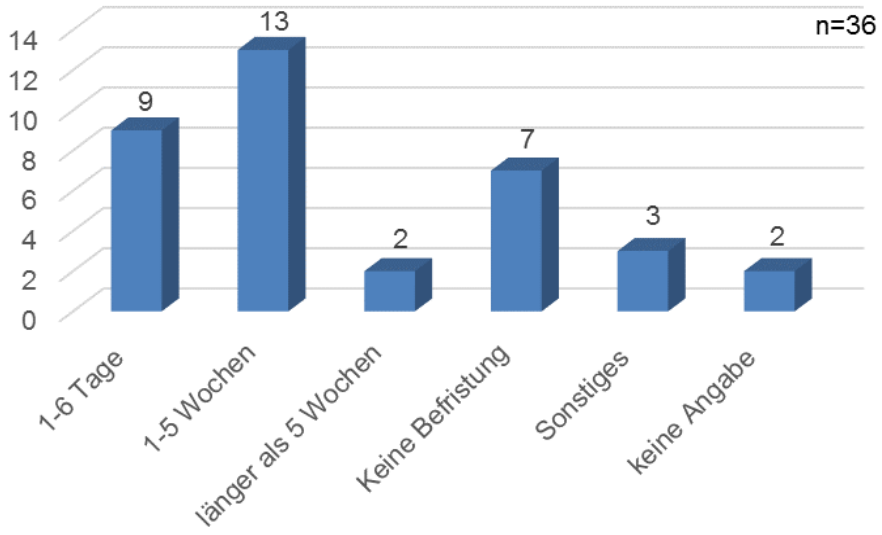
4.1.6 Befristung und Dauer der Datenerhebungsmaßnahme

Die rheinland-pfälzischen Polizeibehörden wurden auch dazu befragt, wie lange die jeweilige Datenerhebungsmaßnahme gemäß § 31 Abs. 1 POG befristet wurde. Beim Großteil der Fälle (22) wurden die Maßnahmen auf nicht länger als fünf Wochen befristet. Lediglich in zwei Fällen erstreckte sich die Befristung auf einen Zeitraum von zwei Monaten. Bei vier Maßnahmen wurde die Datenerhebung bis zum Auffinden der Person und Abklärung der Gefahrensituation (v.a. Suizidandrohung) befristet. In sieben Fällen erfolgte keine zeitliche Begrenzung, da es sich entweder um eine einmalige Datenerhebung, die aufgrund von Gefahr im Verzuge nachträglich durch das OVG bestätigt wurde, oder eine retrograde Datenerhebung handelte. In drei Fällen wurde kein konkreter Zeitraum angegeben. Es wurde darauf hingewiesen, dass Maßnahmen bis zur Ergreifung der suizidgefährdeten Person und zur Überprüfung der Suizidandrohung befristet wurden (Sonstiges). Zu zwei Maßnahmen konnte keine Angabe gemacht werden, warum eine Befristung nicht erfolgte. Folglich wurde in keinem Fall die maximale Frist von drei Monaten von den Polizeibehörden im Evaluationszeitraum ausgeschöpft. Ebenfalls kein Gebrauch wurde von der Möglichkeit gemacht, eine Maßnahme gemäß § 31

809 Hierzu zählen alle durchgeführten Maßnahmen, bei denen es weder organisatorische, zeitliche oder technische Probleme noch bei Probleme bei der Einholung der richterlichen Entscheidung gegeben hat. Da bei einer Maßnahme sowohl Probleme bei der Einholung der richterlichen Entscheidung als auch zeitliche Probleme aufgetreten sind, sind es zehn und nicht elf Maßnahmen mit Problemen.

Abs. 1 POG nach der ersten Befristung noch einmal um maximal zwei Monate zu verlängern.

Abb. 5. Befristung der Dauer der Datenerhebungsmaßnahmen gemäß § 31 Abs. 1 POG[810]



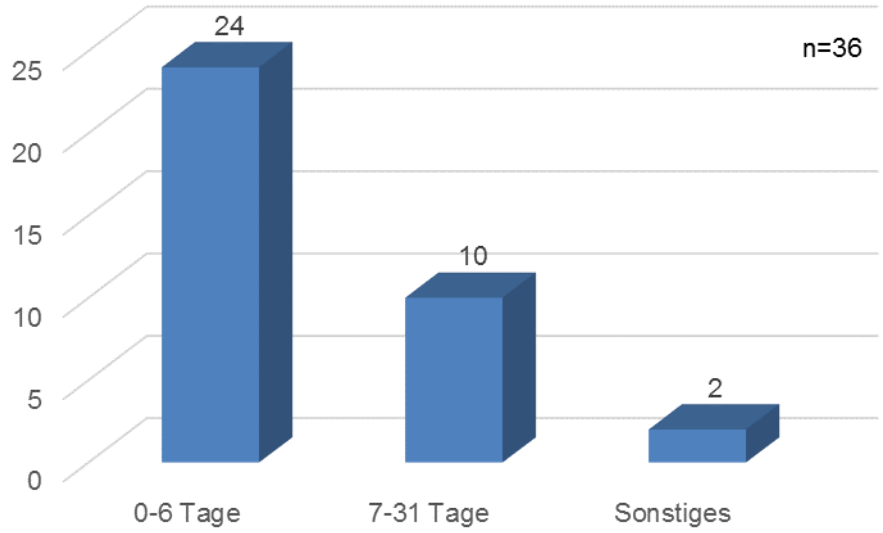
Betrachtet man in diesem Zusammenhang auch noch die tatsächliche Dauer der Datenerhebung, fällt auf, dass diese im Großteil der Fälle (34) nicht mehr als 31 Tage gedauert hat. In 24 Fällen wurden hierfür sogar nur zwischen wenigen Minuten und sechs Tagen benötigt, während zehn Maßnahmen zwischen sieben und 31 Tagen gedauert haben. In zwei Fällen wurden keine konkreten Angaben gemacht, sondern angegeben, dass ausschließlich Verkehrsdaten erhoben wurden bzw. dass es sich um keine andauernde Maßnahme gehandelt hat und lediglich eine Umkehrsuche bei Providern durchgeführt wurde, um herauszufinden, wer zu einem bestimmten Zeitpunkt bei einer bestimmten Nummer angerufen hat.

In diesem Zusammenhang wird deutlich, dass die Polizeibehörden die Datenerhebungsmaßnahmen in der Regel in einem kürzeren als in der Befristung festgelegten Zeitraum abschließen konnten. Auch diese Tatsache deutet auf einen maßvollen Umgang mit den gesetzlich zur Verfügung gestellten Möglichkeiten zur verdeckten Datenerhebung gemäß § 31 Abs. 1 POG hin.

---

810 Das hier angegebene ist n ist größer als 35, da die in einem Fall für zwei Anschlüsse zwei unterschiedliche Befristungen angegeben wurden.

Abb. 6: Tatsächliche Dauer der Datenerhebung gemäß § 31 Abs. 1 POG[811]



Die Polizeibehörden wurden in diesem Zusammenhang auch danach gefragt, aus welchen Gründen die Maßnahme beendet wurde. In 17 Fällen wurde die Beendigung der Gefahrenlage als Grund genannt. In neun Fällen wurden hierzu konkretere Angaben gemacht. So wurde in drei Fällen die Maßnahme beendet, da der Aufenthaltsort der gesuchten Personen ermittelt werden konnte bzw. die gesuchte Person aufgefunden wurde. In je einem Fall konnte der Täter ermittelt bzw. der Verantwortliche in Gewahrsam genommen werden. In einem weiteren Fall gab die Polizeibehörde als Grund für die Beseitigung der Gefahrenlage an, dass der zeitliche Rahmen, für den die Veranstaltung angekündigt war, beendet war. In einem anderen Fall gab es keine weiteren Drohanrufe mehr.

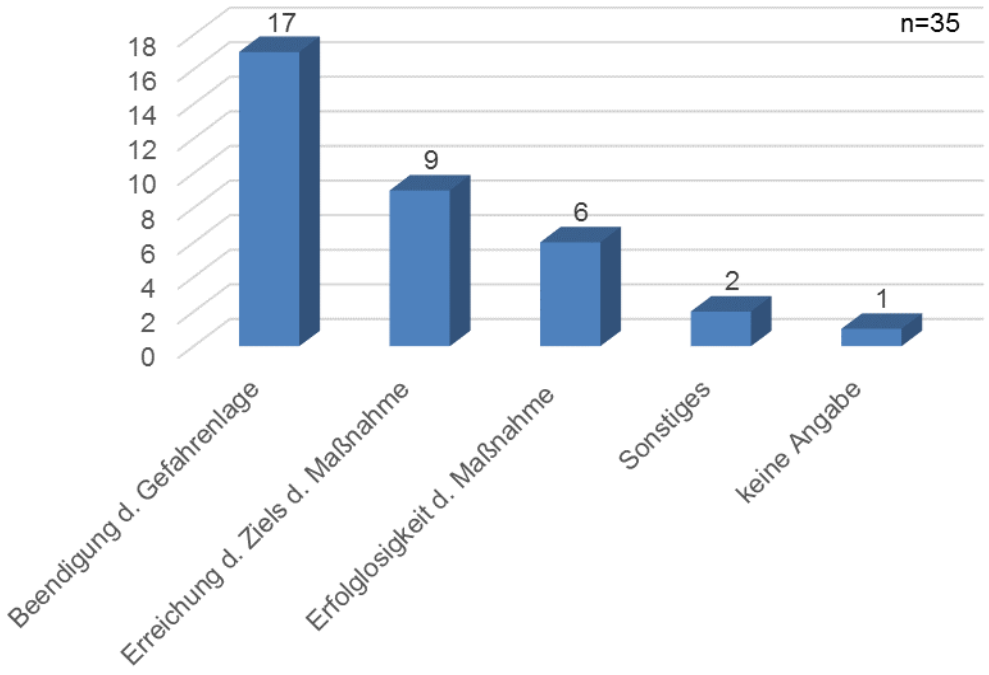
In neun Fällen begründeten die zuständigen Polizeibehörden die Beendigung der Maßnahme damit, dass ihr Ziel erreicht wurde. In acht Fällen konnten die benötigten Daten erhoben werden. So wurden als konkrete Gründe genannt, dass der Anschlussinhaber ermittelt werden konnte, nur ein Drohanruf zurückverfolgt werden sollte, nach der Lieferung der Verkehrsdaten nur noch ein Datenabgleich erfolgte, der Zielsuchlauf abgeschlossen war und es nur um eine retrograde Erhebung mit einem beschränkten Zeitraum ging. In einem Fall wurde die Zielerreichung nicht weiter begründet.

811 Das hier angegebene = n ist größer als 35, da die in einem Fall für zwei Anschlüsse zwei unterschiedliche Befristungen angegeben wurden.

In sechs Fällen wurde die Maßnahme beendet, da sie nicht zum gewünschten Erfolg führte, wobei in fünf Fällen konkrete Gründe genannt wurden. In zwei Fällen wurde von der Polizei ein unbekannter Aufenthaltsort als Grund angegeben. In einem Fall wurde die Maßnahme beendet, da der Betroffene verstorben war. In einem anderen Fall gab die zuständige Polizeibehörde an, dass die Beschlussfrist ablief und keine aktuellen Verkehrsdaten mehr vorhanden waren, weshalb eine Verlängerung des Beschlusses nicht sinnvoll war. In einem weiteren Fall wurde ein ständiger Wechsel des Aufenthaltsorts als Grund für die Beendigung der Maßnahme genannt.

Als sonstige Gründe für die Beendigung wurde noch angeführt, dass der Fall in eine StPO-Maßnahme mit Beschlüssen nach § 100a StPO umgewandelt worden war bzw. in einem anderen Fall eine TKÜ-Maßnahme in ein sich anschließenden Strafverfahren des Generalbundesanwalts bei Bundesgerichtshof geschaltet wurde.

Abb. 7: Gründe für die Beendigung der Datenerhebung gemäß § 31 Abs. 1 POG



Darüber hinaus wurde im Rahmen der Evaluation untersucht, in wie vielen Fällen die Entscheidung, eine Maßnahme gemäß § 31 Abs. 1 POG durchzuführen, wegen Gefahr in Verzug von der Behördenleitung bzw. eines von ihr beauftragten Beamten des höheren Dienstes ohne vorherige Einholung einer richterlichen Entscheidung getroffen wurde. Insgesamt wurde dieser Weg in

13 Fällen beschritten, wobei die zuständigen Polizeibehörden bei elf Maßnahmen konkret angaben, worauf die Annahme einer Gefahr in Verzug gestützt wurde. Genannt wurde in diesem Zusammenhang die Nichterreichbarkeit des OVG (5), allgemein das Vorliegen einer Bedrohungslage (3) sowie das Vorliegen einer Lebensgefahr für einen Säugling (1). Darüber hinaus wurde dieser Weg in zwei Fällen beschritten, da eine Bedrohungslage bestand und die sonstigen vorhandenen Datenerhebungsmöglichkeiten ausgeschöpft waren bzw. nicht zu Verfügung standen. In zwei Fällen wurde dazu keine Angabe gemacht. Dabei variiert der zeitliche Abstand zwischen der Anordnung durch die Behördenleitung und der Nachholung der richterlichen Entscheidung deutlich. Der Unterschied beträgt zwischen zwei Stunden und zehn Tagen, wobei in acht der 13 Fälle die richterliche Entscheidung innerhalb von drei Tagen nachgeholt wurde. In drei Fällen dauerte es länger als drei Tage (vier, sieben und zehn Tage). Zu zwei durchgeführten Maßnahmen konnten hingegen keinen Angaben gemacht werden.

Ergänzend hierzu ist noch darauf hinzuweisen, dass das OVG Koblenz in acht Fällen, in denen die Behördenleitung bzw. ein von ihr beauftragter Beamter des höheren Dienstes die Entscheidung über die Durchführung der Maßnahme getroffen hat, die Anordnung nachträglich bestätigt hat. In vier Fällen wurde die Anordnung durch das OVG nachträglich nicht bestätigt. In einem Fall wurden hierzu keine Angaben gemacht.

Bei der Mehrzahl der durchgeführten Maßnahmen (22) ist von den Polizeibehörden jedoch der „normale Weg“ über das OVG beschritten worden, so dass keine Entscheidung wegen Gefahr in Verzug von der Behördenleitung bzw. eines von ihr beauftragten Beamten des höheren Dienstes getroffen werden musste. Dieses Ergebnis zeigt, dass die Eilkompetenz nicht sehr oft und hauptsächlich dann von der Polizei genutzt wird, wenn das OVG nicht zu erreichen ist.

4.1.7 Weiterverwendung der erhobenen Daten

Ein zusätzliches Prüfkriterium zur Beurteilung der Eingriffsintensität ist die weitere Nutzung der erhobenen Daten durch die Polizeibehörden. Daher wurden die Polizeibehörden danach gefragt, ob und für welche Zwecke sie die gemäß § 31 Abs. 1 POG gewonnenen Daten weiterverwendet haben. Bei der Gesamtauswertung wird deutlich, dass beim Großteil der Fälle (28) diese Daten nicht weiterverwendet wurden – weder zur Abwehr einer anderen dringenden Gefahr noch zur Verfolgung einer besonders schweren Straftat. Lediglich

in sechs Fällen wurden die erhobenen Daten zur Verfolgung einer besonders schweren Straftat im Anschluss an die Maßnahme gemäß § 31 Abs. 1 POG herangezogen. Dabei handelte es sich jeweils um[812]

- Straftaten gegen die persönliche Freiheit in den Fällen der §§ 234, 234a Abs. 1, 2, 239a, 239b, 232 Abs. 3, 4 oder Abs. 5, 233 Abs. 3 StGB, jeweils soweit es sich um Verbrechen handelt,
- Straftaten gegen die sexuelle Selbstbestimmung in den Fällen des §§ 176a Abs. 2 Nr. 2 oder Abs. 3, 177 Abs. 2 Nr. 2 oder 179 Abs. 5 Nr. 2 StGB,
- Mord und Totschlag nach §§ 211, 212 StGB,
- besonders schwerer Fall einer Straftat nach § 29 Abs. 1 S. 1 Nr. 1, 5, 6, 10, 11 oder 13 i.V.m. § 29 Abs. 3 S. 2 Nr. 1 BtMG und
- Kriegsverbrechen nach §§ 8 bis 12 VStGB.

Anhand dieses Ergebnisses wird deutlich, dass die Intensität der Eingriffe durch die verdeckte Datenerhebung gemäß § 31 Abs. 1 POG in der Regel nicht noch dadurch erhöht wird, dass die gewonnenen Informationen für andere Zwecke verwendet werden.

4.1.8 Erfolg der Maßnahme

Um den Erfolg der gemäß § 31 Abs. 1 POG durchgeführten Maßnahmen erfassen zu können, wurden die Polizeibehörden zu verschiedenen Aspekten befragt. Zunächst ging es darum in Erfahrung zu bringen, ob die jeweilige Maßnahme zur Erhärtung eines Gefahren- bzw. Straftatenverdachts beitragen konnte. Beim Großteil der Fälle (24) war dies der Fall, während dies bei elf Maßnahmen verneint wurde. Darüber hinaus wurden die Polizeibehörden danach gefragt, ob durch die Maßnahmen Hinweise auf weitere dringende Gefahren bzw. besonders schwere Straftaten gewonnen werden konnten. Hier ergibt sich bei der Gesamtauswertung ein eindeutiges Bild. Nur in einem Fall traf dies zu, während bei 34 Maßnahmen keinerlei Hinweise gewonnen werden konnten.

Bei der Frage, ob die Maßnahme zur Verhinderung einer Gefahr bzw. Straftat beitragen konnte, zeigt sich hingegen ein differenzierteres Bild. In mehr als

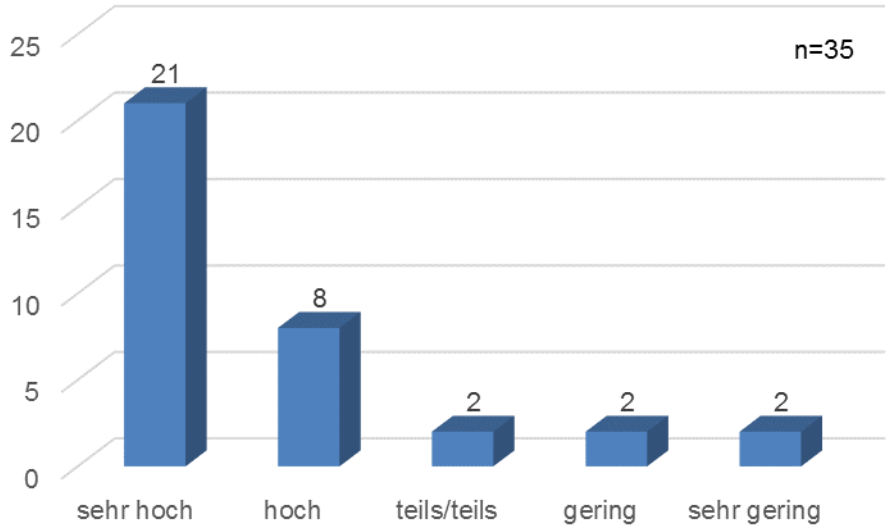
812 In einem Fall wurden keine weiteren Angaben dazu gemacht, zu welchem Zweck die Daten verwendet wurden.

der Hälfte der Fälle (19) gaben die Polizeibehörden an, dass die Maßnahme hierzu einen Beitrag geleistet hat. Hingegen ist dies in elf Fällen nicht eindeutig feststellbar, während in fünf Fällen laut Polizei die Maßnahme keinen Beitrag zur Verhinderung einer Gefahr bzw. einer Straftat leisten konnte.

Im Hinblick auf die Frage, ob die Maßnahme zur Aufklärung einer Straftat beitragen konnte, ergibt sich ein deutlich negativeres Bild. Lediglich in zehn Fällen[813] konnten die nach § 31 Abs. 1 POG durchgeführten Maßnahmen hierzu einen Beitrag leisten. Dagegen wurde in 20 Fällen von den Polizeibehörden darauf hingewiesen, dass die Maßnahme nicht zur Aufklärung einer Straftat beitragen konnte. In fünf Fällen lief das Verfahren noch, während in einem Fall die zuständige Polizeibehörde keine Angaben machen konnte. Insoweit ist allerdings darauf hinzuweisen, dass die Maßnahmen nach dem POG im präventiv-polizeilichen Bereich ergriffen werden.

Abschließend wurden die Polizeibehörden noch danach gefragt, wie sie im konkreten Fall den Nutzen der erhobenen Daten bewerten. Bei der Gesamtauswertung zeigt sich ein eindeutiges Bild. In 29 der 35 Fälle wurde der Nutzen der im Rahmen der Maßnahme gewonnenen Daten als sehr hoch (21) und hoch (8) eingestuft. Hingegen wurde bei vier Maßnahmen auf den geringen (2) bzw. sehr geringen Nutzen (2) der gewonnenen Daten hingewiesen. In zwei Fällen wurden die Daten nur als teilweise nützlich angesehen.

Abb. 8: Nutzen der im Rahmen der Datenerhebung gemäß § 31 Abs. 1 POG gewonnenen Daten



813 In einem Fall gab eine Polizeibehörde an, dass die Maßnahme zur Aufklärung einer Straftat beitragen konnte und dass das Verfahren noch läuft.

Die Bewertungsfrage wurde im Erhebungsbogen für die zweite Phase der Evaluation (2013-2016) wurde zudem um eine offene Frage ergänzt. Somit konnten die Polizeibehörden ihre Bewertung noch weiter erläutern. Diese zusätzlichen Informationen liegen allerdings nur für die zehn Maßnahmen vor, die zwischen dem 01.10.2013 und dem 31.03.2016 durchgeführt wurden. In der mehr als der Hälfte der Fälle wurde von den Polizeibehörden explizit daraufhin gewiesen, dass die Datenerhebung gemäß § 31 Abs. 1 POG die einzige Möglichkeit gewesen sei, die benötigten Informationen zu erhalten (Identifikationen/Lokalisation einer bestimmten Person). Bei den übrigen vier Fällen gaben die Polizeibehörden an, dass mit Hilfe die Maßnahme die zur Aufklärung des Sachverhalts erforderlichen Informationen gewonnen werden konnten (z.B. Standortermittlung des mutmaßlichen Opfers, Erkenntnisse zum Verhalten des Betroffenen und der Kontaktpersonen, Ermittlung des Anschlussinhabers, Erfüllung der polizeilichen Zielsetzung).

Zusammenfassend ist festzuhalten, dass die im Evaluationszeitraum durchgeführten Maßnahmen gemäß § 31 Abs. 1 POG in erster Linie zur Erhärtung eines Gefahren- bzw. Straftatenverdachts beitragen konnten. Teilweise konnten die Maßnahmen auch noch zur Verhinderung einer Gefahr bzw. einer Straftat beitragen. Hingegen wenig hilfreich waren die Datenerhebungsmaßnahmen zur Aufklärung einer Straftat, was jedoch angesichts der gefahrenabwehrrechtlichen Zielsetzung des POG auch nicht verwundern kann. Deutlich erkennbar ist darüber hinaus, dass beim Großteil der Fälle der Nutzen der erhobenen Daten von den Polizeibehörden als sehr hoch bzw. hoch eingeschätzt wird.

4.1.9 Parallele Datenerhebungsmaßnahmen und Stand des Verfahrens

Um die Eingriffsintensität der Maßnahmen nach § 31 Abs. 1 POG besser bewerten zu können, wurde des Weiteren untersucht, ob und – wenn ja – welche weiteren Datenerhebungsmaßnahmen parallel durchgeführt wurden. Hierzu ist zunächst festzuhalten, dass bei über der Hälfte der Fälle (21) keine weiteren Datenhebungsmaßnahmen genutzt wurden, während in 14 Fällen auf zusätzliche Maßnahmen zur Informationsgewinnung zurückgegriffen wurde. Genannt wurden in diesem Zusammenhang:

- Abarbeitung von Zeugenhinweisen aufgrund Presseveröffentlichung (zweimal),
- Anschlussinhaberfeststellung,
- Aufklärung; Personenkontrollen,

- Datenerhebung aus öffentlich zugänglichen sozialen Netzwerken; Maßnahme nach § 31a POG; Wohnungsdurchsuchung (zweimal),
- Einsatz des IMSI-Catcher,
- strafrechtliche Ermittlungen zu schwerem Landfriedensbruch,
- umfangreiche Datenerhebung nach StPO (laufendes Verfahren),
- § 100g StPO Erhebung von Verkehrsdaten des Geschädigten und eines Zeugen (nicht direkt zeitgleich) sowie Handyortung gemäß § 31a POG
- § 31a POG (Handyortung)
- §§ 28, 32 POG
- Erhebung sog. retrograder Verkehrsdaten gemäß §§ 100g StPO

In einem Fall wurden von der zuständigen Polizeibehörde keine Angaben dazu gemacht, welchen Datenerhebungsmaßnahmen parallel durchgeführt worden waren.

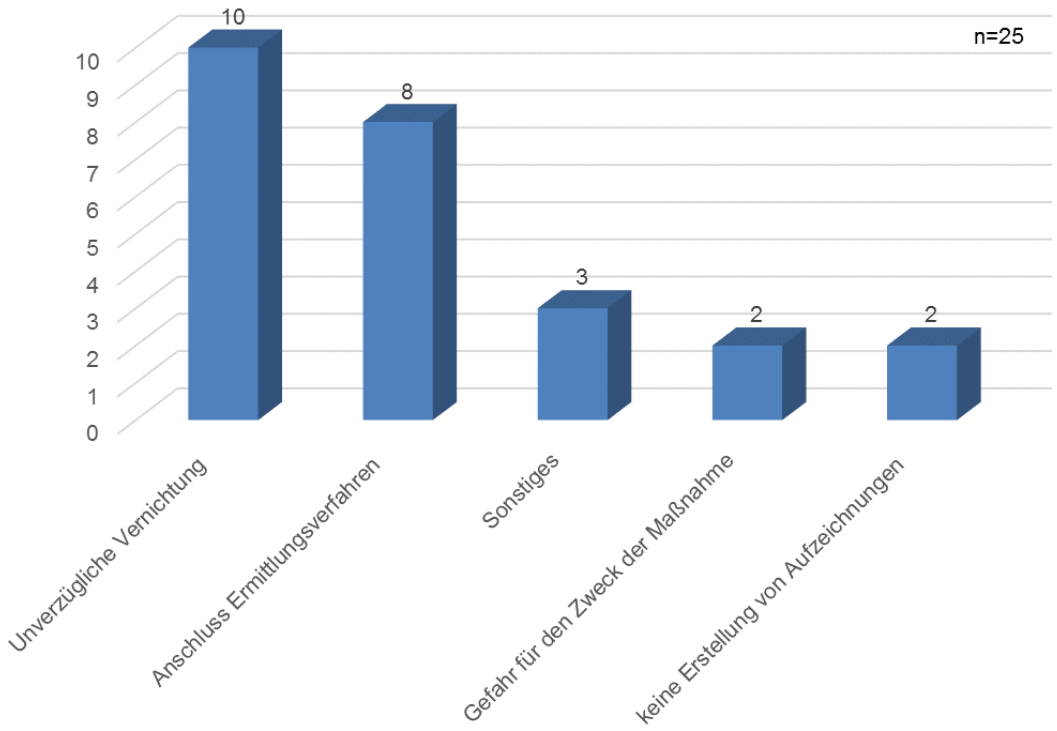
Hinsichtlich des aktuellen Stands des Verfahrens ergibt sich folgendes Bild: In 20 Fällen gaben die Polizeibehörden an, dass das Verfahren an die Staatsanwaltschaft abgegeben worden ist und dort weiter geführt wird. In sechs Fällen war der Vorgang erledigt. In jeweils zwei Fällen wurde angegeben, dass das Verfahren eingestellt worden ist bzw. das Verfahren an die Staatsanwaltschaft abgegeben und mit einer Verurteilung abgeschlossen worden ist. In fünf Fällen konnten die zuständigen Polizeibehörden hierzu keine Angaben machen.

4.1.10 Unterrichtung der betroffenen Personen

Eine ebenfalls wichtige Frage, die im Rahmen der Evaluation untersucht werden sollte, war, ob und wann die Personen, gegen die sich die Maßnahme gerichtet hatte, unterrichtet wurden. Hier zeigt sich, dass in knapp der Hälfte der Fälle (17) keine Unterrichtung erfolgte. Begründet wurde dies hauptsächlich mit der unverzüglichen Vernichtung der personenbezogenen Daten nach Beendigung der Maßnahme (10) sowie mit dem Anschluss eines strafrechtlichen Ermittlungsverfahrens gegen den Betroffenen an den die Maßnahme auslösenden Sachverhalt (8). Je zweimal wurden die Gefahr für den Zweck der Maßnahme sowie keine Erstellung von Aufzeichnungen mit personenbezogenen Daten als Gründe für die nicht erfolgte Unterrichtung genannt. In drei Fällen wurden sonstige Gründe angeführt. Hierzu zählen der Tod des Betroffenen,

die Tatsache, dass der Beschuldigte nicht ermittelt werden konnte sowie der Hinweis, dass die ermittelte Person mehrfach in gleicher oder ähnlicher Weise aufgetreten ist. Anzumerken ist in diesem Zusammenhang, dass in fünf Fällen mehrere Gründe angeführt wurden, warum die betroffenen Personen nicht unterrichtet wurden. In zwei Fällen wurden drei Gründe und in drei weiteren Fällen zwei Gründe für die Unterrichtung genannt.

Abb. 9: Gründe für die nicht erfolgte Unterrichtung der betroffenen Personen[814]



In 18 Fällen wurde den Personen, gegen die sich die Maßnahme richtete, mitgeteilt, dass Daten gemäß § 31 Abs. 1 POG über sie erhoben wurden. In diesen Fällen wurden die Polizeibehörden zudem gefragt, wie lange es gedauert hat, bis sie die Personen nach Abschluss der Maßnahme unterrichtet haben. Dabei wird deutlich, dass diese Unterrichtung durch die zuständige Polizeibehörde in der Regel sehr schnell erfolgte. In 13 Fällen wurde die Person sofort beim Antreffen bzw. telefonisch unmittelbar nach Feststellung des Aufenthaltsortes der Person (10) bzw. einen Tag nach Abschluss der Maßnahme (3) unterrichtet. In einem Fall richtet sich die Datenerhebungsmaßnahme nach § 31

814 Die Anzahl der Begründungen ist höher als die Zahl der Fälle, in denen keine Unterrichtung erfolgte, da in vier Fällen je zwei und in zwei je drei Gründe angegeben wurden.

Abs. 1 POG gegen einen nicht verantwortlichen Dritten gemäß § 7 POG. Diesem war die Maßnahme von Beginn an bekannt, und er hatte schriftlich sein Einverständnis zur Durchführung erklärt. Die formale schriftliche Benachrichtigung erfolgte 22 Tage nach Abschluss der Maßnahme. In drei anderen Fällen hat die zuständige Polizeibehörde 40, 100 bzw. 105 Tage nach Abschluss der Maßnahme die betroffene Person über die Datenerhebung unterrichtet. In einem Fall wurden keine Angaben hierzu gemacht.

Darüber hinaus sieht § 40 Abs. 5 S. 2 POG vor, dass auch sonstige betroffene Personen unterrichtet werden, wenn ein besonders schutzwürdiges Interesse vorliegt.[815] Im Evaluationszeitraum sind zwei sonstige Personen, die durch eine Datenerhebung gemäß § 31 Abs. 1 POG betroffen gewesen waren, im Anschluss an die Maßnahme darüber unterrichtet wurden. In beiden Fällen erfolgte die Unterrichtung am selben Tag bzw. unmittelbar nach Erledigung. In knapp der Hälfte der Fälle (17) wurden nach Angabe der drei Polizeibehörden keine Daten über sonstige betroffene Personen erhoben. In den 15 Fällen erfolgte hingegen keine Unterrichtung, wobei in 13 Fällen die Polizeibehörden hierfür auch eine Begründung nannten. Als Hauptgründe wurden der Anschluss eines strafrechtlichen Ermittlungsverfahrens gegen den Betroffenen an den die Maßnahme auslösenden Sachverhalt sowie die unverzügliche Vernichtung personenbezogener Daten (je 5) angeführt. Weitere Gründe waren

- Gefahr für Leib, Leben oder Freiheit einer Person,
- Gefahr für den Zweck der Maßnahme,
- Notwendigkeit der Erhebung weiterer Daten über die betroffene Person, um diese zu identifizieren (ohne dass dies im Interesse der betroffenen Person geboten erscheint) (zweimal),
- keine Erstellung von Aufzeichnungen mit personenbezogenen Daten sowie
- Sonstiges.

In dem Fall, in dem „Sonstiges“ als Grund angeführt wurde, hat die zuständige Polizeibehörde eine Überprüfung des Anschlussinhabers nach § 112 TKG durchgeführt und dabei festgestellt, dass keine Personen existent waren. Die höhere Anzahl an genannten Gründen im Vergleich zu den durchgeführten Maßnahmen ist dadurch zu erklären, dass in drei Fällen jeweils zwei Gründe genannt wurden. In zwei Fällen erfolgte keine Begründung dafür, warum die Unterrichtung der sonstigen betroffenen Personen unterblieb.

---

815 *Roos/ Lenz*, POG, § 40, Rn. 11.

In einem Fall wurden keine Angaben dazu gemacht, ob sonstige betroffene Personen unterrichtet wurden.

Zusammenfassend ist festzuhalten, dass eine Unterrichtung der Personen, gegen die sich die Maßnahme gerichtet hat, seltener, dafür aber dann relativ zügig erfolgt. In mehr als der Hälfte der Fälle wird auf eine Unterrichtung verzichtet, da die erhobenen personenbezogenen Daten oft unverzüglich vernichtet bzw. keine Aufzeichnungen erstellt werden. Aber auch der Anschluss eines strafrechtlichen Verfahrens stellt einen wichtigen Grund für den Verzicht auf die Unterrichtung der betroffenen Personen dar.

Eine ähnliche Argumentation findet sich auch im Zusammenhang mit der nicht erfolgten Unterrichtung der sonstigen betroffenen Personen, wobei sich hier jedoch grundsätzlich die Frage stellt, ob tatsächlich andere schutzwürdige Interessen vorgelegen haben, die eine Unterrichtung erforderlich gemacht hätten.

4.1.11 Kommentare und Anmerkungen der Polizeibehörden zu den jeweiligen Maßnahmen gemäß § 31 Abs. 1 POG

Zum Abschluss des Fragebogens hatten die Polizeibehörden noch die Möglichkeit, zu dem jeweiligen Fall Kommentare abzugeben bzw. inhaltliche Anmerkungen zu machen. Hiervon machten die Polizeibehörden in drei Fällen Gebrauch. In einem Fall wurde darauf hingewiesen, dass sich die Anordnungskompetenz der Behördenleitung zur schnellen Beseitigung der Gefahrenlage als zielführend erwiesen hat. Ohne die Anordnungskompetenz wäre es möglicherweise zu einem Schaden für Leib oder Leben und bei erheblichen Sachwerten zum Nachteil eines unbestimmten Personenkreises gekommen. In einem anderen Fall gab eine Polizeibehörde an, dass das OVG die Formvorschrift der schriftlichen Anordnung (fernmündliche Vorabanordnung und zu diesem Zeitpunkt noch fehlende schriftliche Anordnung durch LvD) sowie den aus Sicht des Gerichts zu langen Zeitraum (60 Minuten) für die Erhebung von Anrufen rügte.

Im dritten Fall wies die Polizeibehörde darauf hin, dass die gemachten Angaben aus der Erinnerung gemacht wurden, da die Unterlagen nach den datenschutzrechtlichen Bestimmungen bereits gelöscht worden waren.

4.1.12 Darstellung der gemäß § 31b POG durchgeführten Maßnahme

Aufgrund einer Suizidankündigung in einem Gästebucheintrag auf einer Online-Plattform hat das Polizeipräsidium Mainz zur Abwehr einer Gefahr für Leib oder Leben einer Person Auskunft über Nutzungsdaten gemäß § 31b POG verlangt. Der Eintrag erfolgte unter einem Nutzernamen, der die Feststellung der Identität und somit der Gesamtumstände (z.B. Aufenthaltsort der Person, eventuelle Vorerkenntnisse, sozialer Hintergrund) nicht unmittelbar zuließ. Aufgrund der Informationslage gab es kein milderes Mittel als die Feststellung der Nutzungsdaten anhand der vom Administrator der Online-Plattform übermittelten IP-Adresse. Nach Angaben des Polizeipräsidiums handelte es sich somit um den einzigen Ermittlungsansatz.

Die Anordnung der Maßnahme richtete sich gegen eine nach § 4 verantwortliche Person, über die auch tatsächlich Daten erhoben wurden. Dritte waren hingegen von der Datenerhebung nicht betroffen. Bei den erhobenen Daten handelte es sich um Merkmale zur Identifikation des Nutzers. Eine Auskunft über zukünftige Nutzungsdaten wurde nicht angeordnet. Die zuständige Polizeibehörde gab an, dass es keine Probleme im Zusammenhang mit der Durchführung der Maßnahme gegeben habe. Aufgrund von Gefahr in Verzug musste die Maßnahme von einem besonders beauftragten Beamten des höheren Dienstes angeordnet werden. Der Antrag wurde von der Polizeibehörde innerhalb von drei Werktagen an das OVG Koblenz geschickt und nachträglich genehmigt.

Die Polizeibehörde gab an, dass die im Zuge der Maßnahme gemäß § 31b POG gewonnenen Daten anschließend nicht für andere Zwecke verwendet wurden. Zudem wurden parallel zum Auskunftsverlangen keine weiteren Datenerhebungsmaßnahmen durchgeführt.

Aus Sicht des Polizeipräsidiums Mainz konnte die Maßnahme zur Erhärtung eines Gefahrenverdachtes, zur Verhinderung einer Gefahr und zur Aufklärung einer Straftat beitragen. Hingegen konnten durch die Maßnahme keine Hinweise auf weitere dringende Gefahren bzw. besonders schwere Straftaten gewonnen werden.

Diese insgesamt positive Einschätzung der Polizeibehörde kommt auch in der Bewertung des Nutzens der in diesem konkreten Fall erhobenen Daten zum Ausdruck, der als sehr hoch eingestuft wurde. Die Bewertung wurde damit begründet, dass die Datenerhebung zur Klärung des Sachverhaltes führte, da die betroffene Person identifiziert und eine Gefahr für Leib und Leben ausgeschlossen werden konnte. In diesem konkreten Fall handelte es sich um

eine vorgetäuschte Suizidandrohung eines Schülers, der hierfür den Internetzugang seiner Schule genutzt hatte. Das Verfahren wurde an die Staatsanwaltschaft abgegeben und wird dort weitergeführt.

Die Person, gegen die sich die Maßnahme gerichtet hat, wurde einen Tag nach Abschluss der Maßnahme durch die zuständige Polizeibehörde unterrichtet.

Abschließend betonte das Polizeipräsidium Mainz noch einmal, dass aufgrund des ausschließlichen Vorliegens einer IP-Adresse eine Auskunft über Nutzungsdaten gemäß § 31b POG der einzige Ermittlungsansatz zur Identifizierung der gefährdeten Personen und zur Feststellung ihres Aufenthaltsortes gewesen sei, um die drohende Gefahr effektiv abwehren zu können.

4.2 Zentrale Ergebnisse der leitfadengestützten Interviews

Zur Vertiefung und Ergänzung der im Rahmen der quantitativen Erhebung gewonnenen Ergebnisse wurden am Ende des ersten Evaluationszeitraums (2011-2013) leitfadengestützte Interviews mit den Vertretern der Polizeibehörden durchgeführt. Darüber hinaus wurden auf Anregung des Auftraggebers auch Vertreter der Hochschule der Polizei mit in die Untersuchung einbezogen. Ebenfalls befragt wurden die für die zu evaluierenden POG-Maßnahmen zuständigen OVG-Richter, um im Rahmen der Evaluation auch die Perspektive des für die meisten Maßnahmen zuständigen Gerichts berücksichtigen zu können. Zum Ende des zweiten Evaluationszeitraums (2013-2016) wurde hingegen – auch mit Blick auf geringen Fallzahlen – auf eine erneute Befragung der Beteiligten verzichtet. Stattdessen wurden die sechs Polizeibehörden, die Hochschule der Polizei sowie das OVG um die Abgabe einer schriftlichen Stellungnahme gebeten. Aus zeitlichen Gründen war die Hochschule der Polizei nicht in der Lage, die übermittelten Fragen zu beantworten. Das Polizeipräsidium Koblenz gab aufgrund fehlender Anwendungsfälle keine schriftliche Stellungnahme ab und verwies auf die Interviewaussagen aus dem Jahr 2013.

Im Folgenden werden zunächst die zentralen Ergebnisse der leitfadengestützten Interviews mit den sechs Polizeibehörden sowie der Hochschule der Polizei vorgestellt, die entsprechend durch die Ergebnisse der schriftlichen Stellungnahme ergänzt wurden.

4.2.1 Vorteile und Nutzen der gesetzlichen Zurverfügungstellung der Datenerhebungsmaßnahmen

Grundsätzlich sind alle Interviewpartner der Auffassung, dass die gemäß § 100 POG zu evaluierenden Maßnahmen sinnvoll und nützlich seien, auch wenn nicht immer in allen Bereichen Einsatzmöglichkeiten gesehen und bisher für die meisten Maßnahmen Anwendungserfahrungen fehlen würden. Aufgrund der Tatsache, dass es derzeit keine oder nur wenige Anwendungsfälle gebe, könne jedoch nicht darauf geschlossen werden, dass diese Instrumente nicht gebraucht würden. Im Falle von zukünftigen Gefahrenlagen stellten die zu evaluierenden Eingriffsnormen des POG eine wichtige und notwendige Rechtsgrundlage dar, die insbesondere dann zum Tragen komme, wenn kein Anfangsverdacht vorliege und somit nicht auf die entsprechenden StPO-Maßnahmen zurückgegriffen werden könne. Begründet wird diese allgemein positive Einschätzung der hier untersuchten POG-Maßnahmen damit, dass die technischen Möglichkeiten und die elektronische Kommunikation insgesamt zunähmen. Die Maßnahmen seien zudem vor allem bei solchen Fällen nützlich, bei denen in geschlossenen Szenen (z.B. Rocker, Hooligans, Terrorismus) ermittelt werde, da hier oft nur mit Hilfe verdeckter Datenerhebungsmaßnahmen die erforderlichen Informationen gewonnenen werden könnten. Die gesetzliche Zurverfügungstellung der zu evaluierenden Maßnahmen werde auch deshalb als wichtig erachtet, da hiermit ähnliche Möglichkeiten wie in § 4a BKA-Gesetz geschaffen worden seien und man somit nun in der Lage sei, ähnlich wie der Bund zu agieren. Ohne die entsprechenden Maßnahmen sei es oft nicht möglich, lebensrettende Informationen zu erhalten. Alternative Möglichkeiten seien hingegen oft ungenauer und eingriffsintensiver (z.B. Vertrauensperson). Zudem ermöglichten die Maßnahmen die Gewinnung objektiver Ergebnisse (im Gegensatz z.B. zur Befragung von Personen/Zeugen). Somit sind wesentliche Vorteile der zu evaluierenden POG-Maßnahmen ihre Unmittelbarkeit, Schnelligkeit, Zielgerichtetheit sowie Heimlichkeit.

Hauptsächlich genutzt werden von der Polizei bisher die Möglichkeiten gemäß § 31 Abs. 1 POG. Der Nutzen der gesetzlichen Zurverfügungstellung wird insgesamt als hoch eingestuft. Begründet wird dies damit, dass mit Hilfe der Maßnahme bei Vermisstenfällen der Aufenthaltsort der jeweiligen Person festgestellt werden könne, wenn diese unterwegs sei oder sich in den Waldbereich zurückziehe, wobei es weniger um die Gesprächsinhalte, als um die Ermittlung des Aufenthaltsorts einer Person gehe. In seltenen Fällen könne es auch darum gehen, Kontaktdaten oder Gesprächsinhalte zu erfassen, um z.B. herauszufinden, ob tatsächlich die Person selbst oder ein Fremder mit dem Handy kommuniziere. Anwendungsmöglichkeiten sehe man auch im Bereich

der politisch motivierten Kriminalität, da PMK-Straftäter alle existierenden Kommunikationsmöglichkeiten nutzten und sich auf die Überwachungsmaßnahmen der Behörden einstellten und stets damit rechneten, überwacht zu werden. Als Vorteil wird in diesem Zusammenhang auch gesehen, dass Daten verdeckt erhoben werden können, die aufgrund des fehlenden Anfangsverdachts nicht erhoben hätten werden können. Der große Nutzen der Maßnahme gemäß § 31 Abs. 1 POG ergebe sich daraus, dass sie eine schnelle und direkte Gewinnung von wichtigen Informationen ermögliche (z.B. zur Ermittlung des Aufenthaltsorts eines Suizidenten). Alternativ könne man gemäß § 31a POG beim Netzbetreiber den Standort erfragen, dann hätten die Daten jedoch einen zeitlichen Verzug von 30 bis 60 Minuten. Daher sei die Maßnahme nach § 31 Abs. 1 POG die deutlich bessere Maßnahme, wenn die Person in Bewegung ist. Als weiterer Vorteil der Maßnahme wird gesehen, dass die Polizei bereits Erfahrungen mit dieser Maßnahme in der StPO habe, da es sich dort um eine Standardmaßnahme handele. Folglich könne sie auch nach POG schneller zum Erfolg führen.

Der Nutzen der *Wohnraumüberwachung* gemäß § 29 POG wird darin gesehen, dass dadurch wichtige Informationen erhoben werden könnten, die auf anderem Weg nicht gewonnen werden könnten. Als vorteilhaft wird in diesem Zusammenhang angesehen, dass in der Wohnung oder an anderen Orten, die vom erweiterten Wohnungsbegriff erfasst seien, offener kommuniziert werde als beispielsweise am Telefon, da die Zielperson nicht mit einer Überwachung rechne. Gleichzeitig wird betont, dass es sich um eine Ultima Ratio-Maßnahme handele, die nur bei einer geringen Zahl von Sachverhalten in Frage komme (z.B. Extremismus, Terrorismus, gewerbsmäßiger Kinderpornografie, Menschenhandel oder Rauschgiftkriminalität), bei denen jedoch aufgrund des Fehlens eines hinreichenden Tatverdachts noch nicht auf StPO-Maßnahmen zurückgegriffen werden könne. In solchen Fällen sei es wichtig, dass es die POG-Regelung gebe. Als Grund dafür, dass eine Wohnraumüberwachung bisher nicht durchgeführt wurde, wird die hohe Gefahrenschwelle angeführt, wobei dies auch gleichzeitig als sinnvoll erachtet wird. Als weitere Vorteile der Maßnahme werden genannt, dass sie einerseits einen besseren Schutz von Polizeikräften im Einsatz (Aspekt der Eigensicherung) und andererseits eine bessere Lagebewältigung ermögliche, da z.B. bei einer Geiselnahme die Situation in einer Wohnung sicher definiert und damit die Wahrscheinlichkeit erhöht werden könne, Personen in Lebensgefahr zu befreien. Ohne den § 29 POG wäre dies nicht möglich, da sonst eine solche Situation nicht zielgerichtet abgebildet werden könne.

Durch die Einführung der *Quellen-TKÜ* habe der Gesetzgeber auf die technologische Entwicklung und das veränderte Kommunikationsverhalten reagiert. Ohne diese Regelung werde es kaum noch möglich sein, bestimmte Daten zu erheben, da die Kommunikation heute mittlerweile häufig verschlüsselt stattfinde (z.B. WhatsApp, Voice over IP). Infolge der aktuellen Abhörskandale sei davon auszugehen, dass die Nutzung verschlüsselter Kommunikation in Zukunft noch zunehmen werde. Ein möglicher Vorteil der Quellen-TKÜ bestehe darin, dass terroristische Vorbereitungshandlungen wirksam erkannt werden könnten, obwohl die Vorbereitung der Maßnahme eines gewissen zeitlichen Vorlaufs bedürfe.

Eine ähnliche Argumentation gibt es auch im Zusammenhang mit der Einführung der *Online-Durchsuchung*. Auch hier wird darauf hingewiesen, dass der Gesetzgeber auf die technologische Entwicklung reagiert habe, indem er die rechtlichen Grundlagen geschaffen habe, um Daten, die sich z.B. auf einem Computer befinden, verdeckt erheben zu können. Insbesondere bei erhöhten Gefahrenlagen durch terroristische Bedrohungen werde die Maßnahme als notwendiges Instrument angesehen, um die Handlungsfähigkeit der Polizei zu gewährleisten. Aus polizeilicher Sicht besitze die Maßnahme jedoch ein enormes Potential. Theoretisch lasse sich hiermit ein umfangreiches Profil des Betroffenen erstellen, vor allem wenn dieser über vernetzte Kommunikationsgeräte verfügt (z.B. sein Handy mit seinem Tablet und dem PC vernetzt hat). Ebenfalls könnte auf Verbindungsdaten der VoIP-Telefonie zugegriffen werden.

Der Nutzen der *Funkzellenabfrage* im POG werde darin gesehen, dass bei dünner Erkenntnislage mit ihrer Hilfe schnell festzustellen sei, ob jemand ein Störer sein könne. Darüber hinaus ließen sich mit ihr auch Bewegungsbilder erstellen. Zudem könne sie dazu genutzt werden, weitere Erhebungsmaßnahmen vorzubereiten. Grundsätzlich wird es als vorteilhaft erachtet, dass nun analog zur StPO auch eine Ermächtigungsrundlage im POG zur Durchführung einer Funkzellenabfrage geschaffen worden sei. Obwohl derzeit nicht vorstellbar sei, wann diese Maßnahme zum Einsatz kommen könne, sei es denkbar, dass sich in Zukunft Anwendungsfälle ergäben (z.B. im Rahmen einer Vermisstenfahndung, einer Anschlagsdrohung, eines Fußballspiels oder einer Demonstration). Als Vorteil wird auch gesehen, dass mit der Funkzellenabfrage eine Maßnahme eingeführt worden sei, die technisch umsetzbar sei und auch von Nutzen sein könne, wenn es darum gehe, herauszufinden, wo sich eine Person aufgehalten hat.

Im Zusammenhang mit der *Auskunft über Nutzungsdaten* gemäß § 31b POG wird als Vorteil genannt, dass der Gesetzgeber auf die technologische

Entwicklung reagiert und mit der Regelung die Möglichkeit geschaffen habe, diese Daten verdeckt zu erheben. Damit sei es nun auch möglich, auf entsprechende Nutzungsdaten im Telemedienbereich (z.B. Facebook, Internet-Foren, YouTube) zuzugreifen. Ebenfalls als Vorteil wird es gesehen, dass die Maßnahme eine geringere Eingriffsintensität aufweise als z.B. das Mithören oder die Durchsuchung. Sie könnte auch zur Vorbereitung einer Quellen-TKÜ herangezogen werden, wenn z.B. Passwörter für E-Mailkonten oder Cloud-Dienste benötigt würden. Insgesamt wird die gesetzliche Zurverfügungstellung der Maßnahme als sinnvolle und erforderliche Ergänzung zu den StPO-Möglichkeiten gesehen. Einsatzmöglichkeiten böten sich vor allem in solchen Bereichen wie „Ankündigungen von Amokläufen“, in denen nicht sicher gesagt werden könne, ob es sich um einen Trittbrettfahrer oder einen echten Amoktäter handele. Hier bewege man sich im Gefahrenabwehrbereich, da die Tat noch nicht passiert und auch die Schwelle – möglicherweise zum Versuch – noch nicht überschritten sei. Gleiches gelte für Propaganda-Videos, die z.B. volksverhetzende Aussagen oder islamistische Propaganda (Terrorvideos, die Taten verherrlichen und damit auch potentielle Konvertiten anwerben wollen) enthalten. Könnte man nicht auf diese Maßnahme zurückgreifen, wäre dies alles nicht möglich, da man mit den StPO-Maßnahmen alleine nicht weiterkäme.

Auch die gesetzliche Möglichkeit zur Durchführung einer *Rasterfahndung* wird als Vorteil gesehen, da sie z.B. dazu beitragen könne, Ausspähversuche gegen bestimmte Einrichtungen (z.B. im militärischen Bereich) in Erfahrung zu bringen. Die Maßnahme biete darüber hinaus eine gute Möglichkeit, verschiedene Datenquellen auf Übereinstimmungen zu prüfen und festgestellte Störermerkmale abzugleichen. Insbesondere im Zusammenhang mit Anschlagsdrohungen wird die Rasterfahndung als probates Mittel angesehen. Allerdings werde auch davon ausgegangen, dass diese Maßnahme nur in Ausnahmefällen zum Einsatz kommen wird.

4.2.2 Nachteile der gesetzlichen Zurverfügungstellung der Datenerhebungsmaßnahmen und Anwendungsprobleme

Allgemein wird zunächst darauf hingewiesen, dass die Durchführung der zu evaluierenden Maßnahmen ein hohes technisches Know-how und einen großen Personaleinsatz erfordere. Als weitere Probleme werden die komplizierte Gestaltung der betroffenen POG-Normen, die hohen rechtlichen Hürden, die uneinheitliche Gerichtszuständigkeit sowie die fehlende Möglichkeit zur Bestandsdatenabfrage gemäß § 113 TKG gesehen.

Bei der *Wohnraumüberwachung* ergäben sich verschiedene Probleme. So stelle vor allem die Gewährleistung des Kernbereichsschutzes ein potenzielles Problem dar, da nicht klar sei, wann aufgrund der Berührung des Kernbereichs die Aufzeichnung wieder fortgesetzt werden dürfe. Problematisch sei zudem, wie damit umgegangen werden solle, wenn z.B. das Schlafzimmer als besonders privater Raum nicht überwacht werde, jedoch dieser Ort bewusst aufgesucht werde. Die Kernbereichsproblematik verschärfe sich zusätzlich, wenn ein Dolmetscher zum Einsatz kommt, der ohne die erforderliche juristische oder polizeiliche Ausbildung entscheiden solle, wann die Übertragung unterbrochen werden muss. Ein weiteres Problem könne sich bei der Wohnraumüberwachung ergeben, wenn ein Dolmetscher für eine Live-Überwachung nicht zur Verfügung stünde. Zudem wurde der begrenzte Straftatenkatalog moniert.

Als weiterer Nachteil bei der Wohnraumüberwachung wird genannt, dass diese mit einem erheblichen personellen, technischen und zeitlichen Aufwand verbunden sei, da sie von zahlreichen Begleitmaßnahmen flankiert werden müsse. Die Polizei stoße dabei schnell an ihre Grenzen. Bei einem größeren Objekt müssten aufgrund der Vorgabe der Live-Überwachung bis zu 40 Personen im Einsatz sein, die den Wohnraum 24 Stunden am Tag und sieben Tage die Woche live überwachen. Hierbei sei zudem der Einsatz von Fachleuten erforderlich, die an anderer Stelle abgezogen werden müssten. Für den Fall, dass die Störer die Wohnung verlassen, müssten ebenfalls Kräfte vor Ort sein, um ihnen ggf. folgen zu können. Zu den 40 Ermittlern komme somit noch ein großer operativer Stab hinzu. Daneben würden sich taktische Probleme (z.B. was getan werden soll, wenn die Störer die Wohnung nie verlassen und die Batterien der Überwachungsgeräte nicht mehr ausreichen) ergeben. Weitere Probleme, die sich im Zusammenhang mit dieser Maßnahme ergeben könnten, seien die Feststellung, ob die Störer überhaupt im Raum sind, sowie das Herausfiltern von relevanten Informationen, wenn viele Personen anwesend sind und mehrere Gespräche zur gleichen Zeit geführt werden. Problematisch sei bei einer solchen Maßnahme darüber hinaus auch die Erfassung emotionaler Nuancen einer Kommunikation.

Folglich werde genau geprüft, ob es nicht noch andere Möglichkeiten gebe, um an die erforderlichen Informationen zu gelangen. Im Grunde genommen komme die Maßnahme nur dann in Frage, wenn ausreichend Planungszeit zur Verfügung stehe. Daher stelle sich die Frage, ob die Maßnahme im Falle einer gegenwärtigen Gefahr für Leib oder Leben überhaupt umsetzbar wäre.

Im Zusammenhang mit der Maßnahme gemäß *§ 31 Abs. 1 POG* werden ebenfalls verschiedene Nachteile bzw. Probleme gesehen. So wird darauf hingewiesen, dass die klassische Kommunikation zunehmend an Bedeutung verliere und stattdessen neue Kommunikationsmöglichkeiten genutzt würden, die mit Verschlüsselungstechnologien arbeiten. Zudem werde auch die sehr hohe Gefahrenschwelle als Problem gesehen. Darüber hinaus wird es auch als problematisch angesehen, dass es häufig nicht möglich sei, die tatsächlichen Anschlussinhaber zu identifizieren, da diese fiktive Namen benutzen würden. Als Beispiel wird hier auf Erfahrungen mit der Bundesnetzagentur verwiesen, die oftmals Anschlussinhaber liefere, die nicht existieren. Des Weiteren wird ein Problem bei der Zusammenarbeit mit den Providern gesehen. Beispielsweise seien die Provider zur Nachtzeit nicht erreichbar, so dass es schon bei der Einleitung der TKÜ-Maßnahmen zu Verzögerungen komme. Darüber hinaus seien nicht alle Provider kooperationsbereit, so dass es zu Verzögerungen bei der Zustellung der angeforderten Daten kommen könne. Probleme würden sich auch aufgrund der Anlieferungsform der Daten ergeben, da manche Provider diese per Fax schicken, so dass die Daten erst einmal durch die Polizei in ein nutzbares Format gebracht werden müssten. Dies sei dann wieder mit einem Mehraufwand und zeitlichen Verzögerungen verbunden. Des Weiteren wird ein Problem darin gesehen, dass den Providern für die Aufschaltung von TKÜ-Maßnahmen ein Zeitfenster von sechs Stunden zur Verfügung stehe. Dadurch entstehe ein vermeidbarer Zeitverzug, der u.U. zu einem Schadenseintritt führen könne.

Schwierigkeiten können sich auch in den Fällen ergeben, in denen der Beschluss für die TKÜ nicht exakt dem Gesetzeswortlaut entspreche, da die Provider dann eine Schaltung der Maßnahme verweigern.

Des Weiteren wird moniert, dass sich das Antragsprocedere für eine TKÜ nach POG im Vergleich zur StPO-Maßnahme – vor allem in der Anfangsphase – aufgrund der fehlenden Routine komplizierter und aufwändiger gestaltet habe, dies aber auch immer noch sei. Mittlerweile funktioniere die Zusammenarbeit mit dem OVG bei dieser Maßnahme jedoch gut, auch wenn in einigen Fällen kritisch angemerkt wird, dass aufgrund des etwas schwerfälligen Antragsverfahrens und der verzögerten Entscheidung des OVG die vermissten Personen bereits wieder aufgetaucht waren und der Antrag wieder zurückgezogen werden musste. Daher wird die Vermutung geäußert, dass vor allem bei zeitlich dringlichen Entscheidungen aufgrund des höheren Aufwands beim POG versucht werde, die Maßnahme nach StPO zu beantragen und durchzuführen. Das Procedere sei auch deshalb etwas länger – insbesondere wenn es

zu Nachfragen komme –, da die Maßnahme zunächst von einem Polizeibeamten vorbereitet, dann von einem Juristen geprüft und beim OVG beantragt werde. Ein weiteres Problem, das angesprochen wurde, sei, dass Vermisstenfälle zu jeder Tages- und Nachtzeit und eben nicht nur zu den Geschäftszeiten des OVG auftreten könnten. Das OVG wird als relativ hohe Hürde eingestuft, obwohl es sich um einen nicht so intensiven Eingriff handelt. Die Ansiedlung beim Amtsgericht würde bei Vermisstenfällen der Polizei eine schnellere und flexiblere Reaktion ermöglichen. Des Weiteren könnten sich Probleme im Zusammenhang mit der Frage ergeben, wann welche Personen über die verdeckte Datenerhebung zu unterrichten seien.

Bei der *Quellen-TKÜ* (§ 31 Abs. 3 POG) werden ebenfalls mögliche Probleme gesehen. So seien einerseits zwar die rechtlichen Voraussetzungen im POG geschaffen worden, jedoch stehe der Polizei bislang keine Remote-Forensik-Software zur Verfügung, die den verfassungsrechtlichen Anforderungen genüge, so dass diese Maßnahme derzeit technisch nicht umsetzbar sei, obwohl die verschlüsselte Kommunikation zunehmend an Bedeutung gewinne (z.B. Skype, WhatsApp). Darüber hinaus könne es zu datenschutzrechtlichen Problemen kommen, wenn z.B. der Trojaner über umfangreichere Funktionen verfüge als ursprünglich geplant. Auch könnten die Daten von Dritten erst nach deren Identifizierung festgestellt werden und wären dann für die Auswertung nicht verwertbar. Zudem fehle es derzeit am technischen Know-how, um eine solche Software herzustellen (→ Kapitel3.3.4.1, S. 86 f.). Zudem sei die Durchführung dieser Maßnahme mit einem großen zeitlichen und personellen Aufwand verbunden. Die rechtlichen Voraussetzungen seien hier schneller geschaffen worden als die tatsächlichen technischen Gegebenheiten. Moniert wird auch, dass die Möglichkeit, die jeweilige Wohnung zu betreten, um sich z.B. Zugang zum Computer der Zielperson zu verschaffen, bisher nicht rechtlich geregelt sei.

Im Zusammenhang mit der Auskunft über Nutzungsdaten *(§ 31b POG)* wird eine Reihe von Problemen gesehen. Beispielsweise sei es problematisch, dass die jeweiligen Daten sehr schnell – häufig binnen weniger Tage – von den Providern gelöscht würden. Aus diesem Grund sei es erforderlich, die entsprechenden Beschlüsse sehr schnell herbeizuführen und unverzüglich an den Provider heranzutreten. Teilweise würden manche Anbieter die Herausgabe von Nutzungsdaten mit Verweis auf das am Sitz der Konzernzentrale geltende Recht (z.B. Microsoft) verweigern. Bemängelt wird zudem die Blockadehaltung der Provider bei Anfragen sowie die Qualität der Daten. Moniert wird auch, dass oft noch nicht klar sei, was mit Nutzungsdaten eigentlich gemeint sei.

Im Zusammenhang mit der *Online-Durchsuchung* werden ähnliche Probleme wie bei der Quellen-TKÜ gesehen. Auch hier seien einerseits zwar die rechtlichen Voraussetzungen im POG geschaffen worden, jedoch stehe der Polizei bislang keine entsprechende Software zur Verfügung, die den verfassungsrechtlichen Anforderungen genüge, so dass diese Maßnahme derzeit technisch nicht umgesetzt werden könne. Hinzu komme eine Stigmatisierung der Maßnahme durch die Öffentlichkeit aufgrund der Diskussion um den BKA-Trojaner. Darüber hinaus wird auch betont, wie technisch und personell aufwändig die Maßnahme sei. Ein datenschutzrechtliches Problem bestehe darin, dass die Daten von Dritten erst nach deren Identifizierung festgestellt würden und dann für die Auswertung nicht verwertbar seien.

Bei der *Funkzellenabfrage* (§ 31e POG) werden ebenfalls verschiedene Probleme gesehen. So sei beispielsweise eine Funkzelle kein festes Gebilde, sondern könne je nach Witterung oder Tageszeit eine ganz unterschiedliche Ausdehnung aufweisen. Oft sei ungewiss, ob eine Funkzellenabfrage überhaupt zu relevanten Erkenntnissen führen werde. Aufgrund dieser Unsicherheit sei davon auszugehen, dass die Maßnahme nur in seltenen Fällen zum Einsatz kommen werde. Des Weiteren wird kritisch angemerkt, ob die Durchführung dieser Maßnahme eigentlich noch sinnvoll sei, wenn nicht anschließend auf die Bestandsdaten gemäß § 113 TKG zugegriffen werden könne, um die im Rahmen der Funkzellenabfrage gewonnene Kennung einem Besitzer zuzuordnen.

Im Hinblick auf die *Rasterfahndung* (§ 38 POG) sind aufgrund der fehlenden Anwendungserfahrungen sowohl nach POG als auch nach StPO kaum Nachteile bekannt. Es wird lediglich darauf hingewiesen, dass die Auswertung von Massendaten sehr aufwändig und schwierig sei.

4.2.3 Einheitliche Gerichtszuständigkeit für die zu evaluierenden Maßnahmen

Die Interviewpartner wurden auch danach gefragt, ob sie eine einheitliche Gerichtszuständigkeit für die zu evaluierenden POG-Maßnahmen für sinnvoll halten und falls ja, auf welcher Ebene diese angesiedelt werden sollte. Eine einheitliche Gerichtszuständigkeit wird eher befürwortet, wobei allerdings zwei Polizeibehörden darauf hinweisen, dass sich die Aufteilung der Anordnungszuständigkeiten zwischen Amtsgerichten und OVG bewährt habe. Eine weitere Polizeibehörde gibt an, dass eine einheitliche Gerichtszuständigkeit nicht

zwingend erforderlich sei, jedoch die Anordnungszuständigkeit für Maßnahmen gemäß § 31 POG – analog zum § 31a POG – beim Amtsgericht liegen sollte.

Der Vorteil einer einheitlichen Gerichtszuständigkeit bestehe darin, dass diese zu einer Vereinfachung und Beschleunigung des Verfahrens und somit auch zur Wirksamkeit der Maßnahme beitrage. In vielen Fällen komme zudem ein ganzer Maßnahmenkatalog zum Einsatz, so dass man u.U. gezwungen sei, sich mit den jeweiligen Anträgen an unterschiedliche Richter zu wenden. Als Beispiel wird in diesem Zusammenhang der gleichzeitige Einsatz eines IMSI-Catchers (Zuständigkeit Amtsgericht) und einer TKÜ (Zuständigkeit OVG) genannt. Darüber hinaus wird argumentiert, dass es sich bei den Maßnahmen nach POG und StPO um gleichbedeutende Grundrechtseingriffe handele und daher keine Unterschiede hinsichtlich der Zuständigkeit gemacht werden sollten. Um eine Einheitlichkeit bei der Gerichtszuständigkeit bei den hier zu evaluierenden Normen zu erreichen, solle das OVG daher auch zuständig für die Rasterfahndung sein – sofern es bei den übrigen OVG-Zuständigkeiten bleibe.

Kontrovers diskutiert wird darüber, welche Gerichtsbarkeit für die POG-Maßnahmen zuständig sein sollte, ohne dass sich jedoch ein eindeutiges Bild ergibt. Beispielsweise war man sich nicht einig, ob für die Maßnahmen besser die ordentliche Gerichtsbarkeit oder die Verwaltungsgerichtsbarkeit zuständig sein sollte. Für die Verwaltungsgerichtsbarkeit allgemein spreche, dass es sich beim Polizei- und Ordnungsrecht um Verwaltungsrecht handele und das notwendige Know-how zur Bearbeitung dieser Rechtsmaterie dort vorhanden sei.

Im Speziellen wird auch die Bündelung der Zuständigkeiten auf OVG-Ebene positiv bewertet. Begründet wird dies damit, dass die erforderliche Kompetenz dort vorhanden sei und Entscheidungen von einem Kollegialorgan getroffen würden. Zudem würden sich die OVG-Richter nach anfänglichen Schwierigkeiten mittlerweile mit der Materie gut auskennen. Darüber hinaus wird betont, dass die Entscheidung des OVG ein ganz anderes Gewicht als der Beschluss eines Amtsgerichts besitze. Obwohl die Ansiedlung der Maßnahmen beim OVG möglicherweise von der Polizei als „störend“ empfunden werde, werde sie für den Grundrechtsbetroffenen als vorteilhafter angesehen, weil die Anordnung eingriffsintensiver Maßnahmen durch höhere Gerichte (wie z.B. das OVG) als sinnvoll anzusehen sei.

Allerdings wird auch daraufhin gewiesen, dass eine Anordnung nach § 100a StPO einen gleichwertigen Grundrechtseingriff darstelle, diese Entscheidung jedoch beim Amtsgericht getroffen werde. Einerseits sei es ver-

ständlich, die Anordnungskompetenz für die Wohnraumüberwachung aufgrund ihrer Eingriffsintensität auf einer höheren Ebene anzusiedeln. Andererseits müssten jedoch Entscheidungen z.B. zu Maßnahmen gemäß § 31 Abs.1 POG nicht zwingend vom OVG getroffen werden. Als Nachteil der OVG-Zuständigkeit wird die damit verbundene Postulationspflicht gesehen. Zudem wird bemängelt, dass das OVG außerhalb der Regeldienstzeit nicht zu erreichen sei, da es keine Bereitschaftsregelung gebe.

Als Vorteil einer Zuständigkeit der ordentlichen Gerichtsbarkeit wird angeführt, dass die Polizei besonders im Umgang mit den Amtsgerichten geübt sei, da dort bereits viele Maßnahmen beantragt würden und auch die jeweiligen Ansprechpartner bekannt seien. Die erforderliche Kompetenz sei auch am Amtsgericht vorhanden, da hier bereits über entsprechende StPO-Maßnahmen entschieden werde, die im Vergleich zu den POG-Maßnahmen als nahezu identisch eingestuft werden. Ebenfalls positiv hervorgehoben wird die gute Erreichbarkeit und die entsprechende Sachnähe der Amtsrichter, da sie rund um die Uhr erreichbar seien und sich häufiger als das OVG mit solchen Themen beschäftigen würden. Die Ortsnähe wird jedoch auch als möglicher Nachteil gesehen, da vermutet wird, dass aufgrund der engen Kontakte zur Polizei u.U. Anträge seltener abgelehnt würden. Gegen eine Ansiedlung der Maßnahmen beim Amtsgericht spreche auch, dass es mit der Anwendung gefahrenabwehrrechtlicher Maßnahmen nicht so vertraut sei und stattdessen versuche, auf die entsprechenden StPO-Maßnahmen zurückzugreifen, da das POG nicht zum Alltagsgeschäft der Amtsrichter gehöre. Die Parallelität der Normen wird in diesem Zusammenhang ebenfalls als Problem gesehen.

4.2.4 Kompensationen der Benachrichtigungspflichten durch Unterrichtung des LfDI bzw. des Landtags

Die Vertreter der sechs Polizeibehörden sowie der Fachhochschule der Polizei wurden auch danach gefragt, wie sie den Vorschlag beurteilen, dass in Fällen, in denen eine Unterrichtung aufgrund der Ausnahmen in § 40 Abs. 5 und 6 POG unterbleibt, jedoch zahlreiche personenbezogene Daten erhoben wurden, anstelle der Unterrichtung des/der Betroffenen darüber öffentlich zu informieren ist bzw. der Landesdatenschutzbeauftragte (LfDI) oder das Parlament nach Abschluss der Maßnahme, wenn ein Ermittlungserfolg nicht mehr gefährdet werden würde, zu unterrichten sind.

Der Vorschlag wird von den Interviewpartnern – auch innerhalb der jeweiligen Polizeibehörden – sehr intensiv diskutiert, ohne jedoch dabei zu einem

eindeutigen Ergebnis zu kommen. Weitgehend Einigkeit herrscht darüber, dass eine öffentliche Information als Kompensation der Unterrichtung abgelehnt wird. Hingegen wird der Vorschlag, den LfDI bzw. den Landtag zu unterrichten, durchaus als eine Alternative zu den bisherigen Benachrichtigungspflichten gesehen. Allerdings wird die vorgeschlagene Kompensation von einigen Interviewpartnern auch kritisch gesehen. So wird es als problematisch erachtet, dass mit dem LfDI und dem Landtag weitere Institutionen Zugang zu den erhobenen Daten erhalten würden und sich damit Geheimhaltungsprobleme ergeben könnten. Stattdessen wird vorgeschlagen, das jeweils zuständige Gericht über die Beendigung und das Ergebnis der jeweiligen Maßnahme zu informieren, da es sich um eine neutrale Instanz handele und das Verfahren damit zu einem sauberen Abschluss gebracht werden könne.

Dieses Gericht sollte auch entscheiden, in welchem Fall eine Unterrichtung unterbleiben könne. Moniert wird darüber hinaus, dass bei einer Übermittlung personenbezogener Daten im Zusammenhang mit der vorgeschlagenen Unterrichtung des Landtags oder des LfDI die polizeiliche Maßnahme gefährdet werden könnte. Eine Mitteilung personenbezogener Daten sei aber auch deshalb nicht sinnvoll, da diese z.T. gar nicht vorliegen würden (siehe Maßnahmen gemäß § 31 POG) und somit erst recherchiert werden müssten, um sie z.B. dem LfDI mitteilen zu können. Dies würde aber die Eingriffsintensität der Maßnahme zusätzlich erhöhen. Kontrovers wurde in diesem Zusammenhang auch diskutiert, wie eine solche Unterrichtung (detaillierte Information oder anonyme Statistik) konkret aussehen sollte. Im Ergebnis wurde der Benachrichtigung des Betroffenen Vorrang eingeräumt, da eine Unterrichtung keine „Feigenblattlösung“ sein dürfe und, sofern der Betroffene feststehe, dieser auch unterrichtet werden solle.

Der Nutzen einer anonymisierten Statistik wird dagegen angezweifelt. Befürchtet wird zudem, dass durch die alternative Benachrichtigungspflicht polizeiliche Taktiken enthüllt werden könnten. Aus Sicht des Datenschutzes sollte das bisherige Verfahren beibehalten werden. Wenn nach zwölf Monaten keine Unterrichtung erfolgt ist, werde das OVG benachrichtigt. Nach mehrmaliger Zurückstellung der Unterrichtung werde der LfDI darüber informiert.

Darüber hinaus wird angemerkt, dass eine ersatzweise Unterrichtung des LfDI oder des Parlamentes ohnehin nur sinnvoll sei, wenn diese auch über die Gründe der unterbliebenen Unterrichtung des Betroffenen informiert werden würden. Hierzu müsste dann aber der Sachverhalt mitgeteilt werden. Kritisch hinterfragt wird zudem der Sinn und Zweck einer solchen Unterrichtung. Eigentlich solle eine Benachrichtigung einen nachträglichen Rechtsschutz für die

Betroffenen ermöglichen. Unklar sei daher, welche Rolle der LfDI oder der Landtag in diesem Zusammenhang spielen solle. Des Weiteren wird darauf verwiesen, dass bei TKÜ-Maßnahmen sowie bei der Wohnraumüberwachung bereits eine automatisierte Unterrichtung des LfDI über das Zentrale Verfahrensverzeichnis der Polizei (ZVPol) erfolge. Hierüber erhalte er Informationen dazu, wie lange eine Maßnahme gedauert habe und wann die erhobenen Daten gelöscht worden seien. Hinsichtlich des Vorschlags einer alternativen Benachrichtigung des LfDI oder des Landtags wird darauf hingewiesen, dass damit ein erhöhter Protokollierungsaufwand für die Polizei verbunden wäre. Darüber hinaus wird angezweifelt, dass sich der Vorschlag umsetzen lasse, da der Gesetzgeber großen Wert darauf lege, die Betroffenen – wenn möglich – immer zu benachrichtigen.

Im Zusammenhang mit den Benachrichtigungspflichten wird darüber hinaus allgemein auf eine Reihe von Problemen hingewiesen. So wird darauf verwiesen, dass sich durch die direkte Benachrichtigung die Wahrscheinlichkeit einer Klage erhöhe. Zudem könne eine Unterrichtung zu einer erheblichen Verunsicherung der Betroffenen führen, da diese sich fragen würden, wann welches Handy aus welchem Grund abgehört wurde, wann diese Maßnahme angewendet wurde und welchen Sinn diese hatte. Somit könnte insbesondere die Benachrichtigung der als unbeteiligte Dritte eingestuften Personen für mehr Verwirrung sorgen als dies zur Aufklärung beitrage. In diesem Zusammenhang wird darauf hingewiesen, dass die Benachrichtigungspflichten gegenüber den betroffenen Personen gemäß § 40 Abs. 5 POG in anderen Ländern bereits dazu geführt habe, von der Anwendung der Maßnahme Abstand zu nehmen. Kritisch angemerkt wird dabei, dass die Neuregelung dieser Berichtspflicht sehr weit gefasst sei und somit in manchen Fällen die polizeiliche Arbeit – auch aus taktischer Sicht – erschweren könne. Ebenfalls angesprochen wird der hohe Arbeitsaufwand, der mit der Benachrichtigung verbunden sei. Als problematisch wird es gesehen, dass sich bestimmte Zielpersonen, die über die Maßnahme unterrichtet wurden, auf die Überwachung der Polizei einstellen würden.

4.2.5 Optimierungsmöglichkeiten aus Sicht der Polizeibehörden

Die Interviewpartner wurden auch danach gefragt, welche konkreten Optimierungsmöglichkeiten sie im Zusammenhang mit den zu evaluierenden POG-Eingriffsnormen sehen. Allgemein wurde darauf hingewiesen, dass die Verständlichkeit und die Lesbarkeit der Normen verbessert werden sollte, da ihre komplizierte Ausgestaltung – auch aufgrund der Vielzahl an Verweisen – die

Anwendung der Regelungen deutlich erschwere. Diese Verweise würden dazu führen, dass die rechtliche Materie unübersichtlich und schwer zu erfassen sei. In diesem Zusammenhang wird darauf verwiesen, dass der Polizei nicht immer klar sei, welche Normen zur Datenerhebung herangezogen werden müssen. Insbesondere bei Ad-hoc-Maßnahmen, bei denen es um Gefahren für Leib und Leben gehe, sei aufgrund des Zeitfaktors eine Auseinandersetzung mit den Regelungen schwierig. Ebenfalls Nachbesserungsbedarf wird bei den Unterrichtungspflichten gesehen. Zum einen werden eine längere Frist bei der Benachrichtigung und zum anderen eine Ergänzung der Gründe für die ausbleibende Unterrichtung gefordert. So sollte eine Unterrichtung auch unterbleiben, wenn die Sicherheit des Bundes und eines Landes gefährdet sei. Konkretisierungsbedarf wird auch beim Begriff des Kernbereichs privater Lebensgestaltung gesehen, da dieser klarer gefasst und besser dargestellt werden sollte. Darüber hinaus sollte bei allen beantragten Maßnahmen gewährleistet sein, dass die Gerichte zügig über die Anträge entscheiden.

Hinsichtlich der *Wohnraumüberwachung gemäß § 29 POG* wurde es als sinnvoll erachtet, die rechtliche Möglichkeit einer technischen Aufzeichnung zu schaffen, um damit die Arbeit der Polizei zu erleichtern. Mit Blick auf den Kernbereichsschutz wurde darauf verwiesen, dass entsprechende Gesprächspassagen problemlos im Nachgang gelöscht werden können. Hingegen stelle es sich bei Live-Überwachungen deutlich schwieriger dar, den Kernbereichsschutz im vollen Umfang zu gewährleisten, vor allem wenn ein Dolmetscher ohne juristischen Hintergrund zum Einsatz komme. Aufgrund ihrer großen Kernbereichsrelevanz sei diese Maßnahme zurzeit kaum umsetzbar. Ein weiterer Aspekt, der im Zusammenhang mit § 29 POG angesprochen wurde, sei eine mögliche Erweiterung des Absatzes 7, der den Einsatz technischer Mittel zum Schutz der bei einem polizeilichen Einsatz tätigen Personen regele. Angeregt wird hier, den Absatz so zu modifizieren, dass er auch für die Durchführung kleinteiliger bzw. punktueller Maßnahmen angewendet werden könne, z.B. wenn eine SEK-Einheit verdeckt Daten aus einer Wohnung erhebt, die für einen schnellen und sicheren Zugriff benötigt würden (z.B. der genaue Aufenthaltsort der sich in der Wohnung befindlichen Personen).

Auch bei der *präventiven TKÜ gemäß § 31 Abs. 1 POG* ergeben sich Optimierungsmöglichkeiten. So wird es als notwendig erachtet, dass der Gesetzgeber verbindliche Vorgaben für die Datenübermittlung durch die Provider (z.B. einheitliches Dateiformat [elektronische Übermittlung und nicht per Fax], unverzügliche Übermittlung) schaffe, damit die Zurverfügungstellung der Daten beschleunigt und die polizeiliche Arbeit nicht mehrere Tage oder Wochen behindert werde. Neben dieser stärkeren Akzentuierung der Pflichten seien

auch Sanktionen bei Nichteinhaltung denkbar. Darüber hinaus wird angeregt, die Gefahrenschwelle an der Schwere der in der Norm geregelten Eingriffe zu orientieren. So solle bei der Erhebung der Inhaltsdaten die Anforderung einer gegenwärtigen Gefahr beibehalten werden, da hier ein vergleichsweise schwerer Grundrechtseingriff vorliege, während bei den übrigen Erhebungsmöglichkeiten (aktuelle Verkehrsdaten sowie retrograde Verkehrsdaten) eine dringende Gefahr ohne Gegenwärtigkeitsbezug ausreichen sollte. Ebenfalls Optimierungsbedarf wird beim § 31 Abs. 7 POG gesehen, der die Kennzeichnung und Weiterverwendung der gewonnenen Daten regelt. Der Verweis auf den § 29 Abs. 5 POG führe in der Praxis zu Irritationen, da dort Bezug auf die Wohnraumüberwachung genommen werde. Daher solle hier eine klarere Regelung geschaffen werden. Zudem wird vorgeschlagen, dass für die Anordnung von TKÜ-Maßnahmen – wie bei der Identifizierung und Lokalisierung von mobilen Telekommunikationsendgeräten gemäß § 31a POG – zukünftig auch das jeweilige Amtsgericht zuständig sein sollte.

Im Zusammenhang mit dem *§ 31 Abs. 3 POG (Quellen-TKÜ)* wird darauf hingewiesen, dass die technischen Voraussetzungen geschaffen werden müssten, damit die Maßnahme auch durchgeführt werden kann. Darüber hinaus solle das Recht, die Wohnung der Zielperson zu betreten und ggf. nach dem entsprechenden Gerät zu suchen, explizit in die Norm aufgenommen werden, da es ist bislang unklar sei, ob dies durch die richterliche Anordnung abgedeckt sei.

Bei *§ 31b POG* wird angeregt, die Zuständigkeit für die Anordnung der Maßnahme nicht beim OVG sondern auf einer niedrigeren Ebene anzusiedeln. Darüber hinaus könnte auch die Gefahrenschwelle abgesenkt werden.

Im Zusammenhang mit der *Online-Durchsuchung (§ 31c POG)* wird vorgeschlagen, dass – analog zum § 29 Abs. 7 POG – eine „Gefahr in Verzug“-Regelung ergänzt werden sollte.

Für die *Funkzellenabfrage (§ 31e POG)* wird eine Vereinheitlichung der Bedingungen für die Datenanlieferung durch den Provider als notwendig erachtet. Zudem stelle sich die Frage, ob es aufgrund der fehlenden landesgesetzlichen Regelung für die Bestandsdatenauskunft nicht zu einer Entwertung der Maßnahme komme, da derzeit nur z.B. die Kennung oder Nummer eines Mobilfunkgerätes erhoben werden dürfe, nicht jedoch die Daten zum Anschlussinhaber (z.B. Name, Adresse). Dies betrifft jedoch auch andere POG-Normen (z.B. § 31 POG). Durch diese Regelungslücke werde die Polizei in ihrer Handlungsfähigkeit beschränkt. Daher sollte hier eine gesetzliche Regelung geschaffen werden.

Hinsichtlich der *Vorratsdatenspeicherung* wird auf die Notwendigkeit einer ausreichend langen und einheitlichen Speicherungsdauer von mindestens sechs Monaten hingewiesen, da die Verfügbarkeit der Daten auch für die POG-Normen relevant sei. Allerdings müsse diese Regelung auf Bundesebene erfolgen. Des Weiteren wird eine Verschärfung der gesetzlichen Regelungen in Bezug auf die Anschlussinhaber gefordert, um zu verhindern, dass fiktive Personen als Inhaber eines Anschlusses eingetragen werden können. Die ehemalige Praxis, bei solchen Anschlussregistrierungen bzw. dem Kauf von Mobilfunkgeräten einen Personalausweis zu verlangen, sei sinnvoll gewesen, werde jedoch durch die Möglichkeit erschwert, SIM-Karten online zu kaufen.

4.2.6 Weiterer Regelungsbedarf aus Sicht der Polizeibehörden

Zum Abschluss wurden die auch danach gefragt, ob es noch weitere Datenerhebungsmaßnahmen gibt, die gesetzlich geregelt werden sollten. Hier wurde z.B. auf die Schaffung der Möglichkeit, *automatische Kennzeichenlesesysteme* einzusetzen, hingewiesen, die als ein taugliches Instrument angesehen würden, wie ihr erfolgreicher Einsatz im repressiven Bereich sowie in anderen Bundesländern zeige. Bei hoher Gefahrenlage werde ebenfalls der Einsatz einer *automatischen Gesichtserkennung* für sinnvoll erachtet. Ebenfalls Regelungsbedarf wird im Zusammenhang mit der *Finanzermittlung* gesehen, da es beispielsweise bei Bankauskünften im Bereich der organisierten Kriminalität schwierig sei, an die Auskünfte zu Kontodaten (z.B. bei Western Union oder allgemeinen Transaktionen) zu gelangen, wenn die Maßnahme nach dem POG erfolge. Gefordert wird zudem, dass die *E-Mails im Entwurfsstadium* klar der Kommunikation zugeordnet würden. Darüber hinaus wird ein Regelungsbedarf bei der *Bestandsdatenauskunft* (siehe § 113 TKG) im POG gesehen, die derzeit rechtlich nicht möglich sei. Hier bestehe eine Regelungslücke, da die Polizei im Rahmen der Gefahrenabwehr mit einer Einzelanfrage momentan nicht in Erfahrung bringen dürfe, wem z.B. eine Festnetztelefonnummer gehört. Des Weiteren wird zur Erhöhung der Handlungssicherheit die Schaffung einer spezialgesetzlichen Regelung für offene Datenerhebungsmaßnahmen (z.B. Bodycam, Drohnen, Kennzeichenlesesysteme) angeregt, die grundsätzlich zulässig seien, jedoch in § 28 Abs. 2 POG technikneutral genannt sein.

4.2.7 Bewertung des OVG Koblenz

Um einen Eindruck gewinnen zu können, wie die Zusammenarbeit zwischen den Polizeibehörden und dem OVG funktioniert und wo ggf. Probleme bestehen, wurde auch die Perspektive des OVG mit in die Evaluation einbezogen. Hierzu wurde der für die POG-Maßnahmen zuständige 7. Senat gebeten, eine Stellungnahme zu folgenden Themenbereichen abzugeben:

- Vorgehen bei Anträgen zur Durchführung der Datenerhebungsmaßnahmen,
- mögliche Probleme beim derzeitigen Beantragungsverfahren,
- Qualität der Anträge,
- Anwendungserfahrungen und Optimierungsmöglichkeiten,
- einheitliche Gerichtszuständigkeit für die POG-Maßnahmen.

Hinsichtlich des Vorgehens bei Anträgen zur Durchführung der Datenerhebungsmaßnahmen gemäß § 100 POG gibt das OVG an, dass bereits vor Einreichung des schriftlichen Antrags eine telefonische Kommunikation mit der jeweiligen Polizeibehörde stattfinde, da eine Entscheidung regelmäßig eilbedürftig sei. Sofern noch Fragen zum Sachverhalt (v.a. zum Bestehen einer gegenwärtigen Gefahr und zur Notwendigkeit der Eingriffsmaßnahme) bestehen würden, finde ebenfalls eine telefonische Kommunikation mit dem Sachbearbeiter der jeweiligen Polizeibehörde oder mit dem für die Antragstellung zuständigen Juristen statt. Die Beantragung der gerichtlichen Anordnung erfolge analog zu § 81 Abs. 1 VwGO schriftlich. Zudem gelte beim OVG gemäß § 67 Abs. 4 VwGO Vertretungszwang. Mittlerweile gebe es bei der Beantragung der Maßnahmen keine Probleme mehr, da die Abgrenzung zum Amtsgericht klar und den Polizeibehörden der Vertretungszwang bekannt sei. Bei der Bearbeitung der Anträge durch das OVG würden keine Probleme auftreten. Die Anträge würden sorgfältig geprüft, so dass es gelegentlich zu Nachfragen im Zusammenhang mit den Tatbestandsvoraussetzungen und der Notwendigkeit der Durchführung der Datenerhebungsmaßnahme bei den Polizeibehörden komme.

Insgesamt würden die Zusammenarbeit mit den Polizeibehörden sowie die Qualität der gestellten Anträge vom OVG als gut bewertet. Sofern es zu Nachfragen komme, würden diese umgehend beantwortet. Nach Einschätzung des OVG sei die Zahl der gestellten Anträge für die in § 100 POG genannten Maßnahmen nicht groß, da die gesetzlichen Anforderungen für die verdeckten Ermittlungsmaßnahmen aufgrund der Eingriffsintensität sehr hoch seien. Dabei

seien sich die Polizeibehörden ihrer Verantwortung beim Persönlichkeitsschutz und beim Recht auf informationelle Selbstbestimmung bewusst und würden keine Anträge „ins Blaue hinein“ stellen.

Optimierungsmöglichkeiten im Zusammenhang mit den Regelungen zu den Datenerhebungsmaßnahmen werden vom OVG in einer Klarstellung des § 39a Abs. 4 hinsichtlich des Prüfumfangs und der Sachleitungsbefugnis gesehen, da nicht ganz klar sei, wie weit die Sachleitungsbefugnis reichen solle. Nach Auffassung des OVG könne es nicht Aufgabe des Gerichts sein, alle erhobenen Daten auf ihre Kernbereichsrelevanz zu überprüfen, da es sich hierbei um eine Verwaltungsaufgabe handele, die zunächst von der Polizei wahrzunehmen sei. Zudem wird darauf hingewiesen, dass das OVG in zweiter Instanz für die Gewährung des nachträglichen Rechtsschutzes bei Unterrichtungen gemäß § 40 Abs. 5 POG zuständig sei, wodurch dasselbe Gericht zunächst die Sachleitungsbefugnis und anschließend die Kontrollbefugnis besitze. Dies spreche dafür, die Sachleitungsbefugnis einschränkend zu verstehen. Somit bedeute die Überprüfung der Realisierung der gegebenen Vorgaben für die Prüfung der Kernbereichsrelevanz nicht, dass das OVG die Daten selbst auszuwerten habe, sondern dies primär durch die Polizeibehörden in eigener Verantwortung erfolgen solle (→ Kapitel 3.3.10.4, S. 133 ff.). Die Aufgabe des OVG könne in diesem Zusammenhang lediglich darin bestehen, allein nach Vorlage durch die Polizei bei tatsächlichen Anhaltspunkten auf Kernbereichsrelevanz eine Überprüfung durchzuführen und ggf. eine Entscheidung über die Löschung und ein Verwertungsverbot zu treffen. Für eine solche Kontrolle wird daher angeregt, die Technik zur Markierung von kernbereichsrelevanten Stellen des LKA, die bereits im StPO-Bereich zum Einsatz komme, auch für die POG-Maßnahmen zu nutzen.

Ebenfalls Optimierungsbedarf sieht das OVG bei der Überwachung des E-Mail-Verkehrs, da nicht klar sei, ob diese auf § 31 Abs. 1 POG gestützt werden könne.

Das OVG spricht sich zudem für eine einheitliche Gerichtszuständigkeit für die Datenerhebungsmaßnahmen nach dem POG aus. Die Anordnungskompetenz für die zu evaluierenden Normen sollte in der Verwaltungsgerichtsbarkeit angesiedelt werden, da es hier um klassische polizeirechtliche Fragen gehe (z.B. das Bestehen einer gegenwärtigen Gefahr). Jedoch wird in diesem Zusammenhang auch angemerkt, dass nicht für jede Maßnahme die Zuständigkeit des OVG erforderlich gewesen wäre und stattdessen eine Ansiedlung bei den Verwaltungsgerichten ausgereicht hätte (z.B. bei Vermisstensachen). Die Notwendigkeit, weitere Datenerhebungsmaßnahmen im POG zu regeln, sieht das OVG nicht.

5. Zusammenfassende Bewertung

5.1 Allgemeiner Teil

In einer Gesamtbewertung ist die gesetzliche Zurverfügungstellung der gemäß § 100 POG zu evaluierenden Datenerhebungsmaßnahmen als sinnvoll zu erachten. In Anbetracht dessen, dass noch nicht alle Maßnahmen zum Einsatz gekommen sind, fehlen teilweise praktische Erfahrungen, die empirisch hätten erhoben und bewertet werden können. Aus einem bislang nicht erfolgten Einsatz einer gesetzlich zur Verfügung stehenden Eingriffsmöglichkeit wird nicht auf die Entbehrlichkeit der betreffenden gesetzlichen Ermächtigung geschlossen werden können. Die notwendige Entwicklung der seitens der Polizeibehörden benötigten, bislang noch nicht für alle zugelassenen Eingriffe vorhandenen technischen Voraussetzungen wird die Polizeibehörden in Zukunft in die Lage versetzen, bei entsprechend schwerwiegenden Gefahrenlagen noch flexibler reagieren zu können. Das evaluierte Eingriffsinstrumentarium stellt für die Polizeibehörden eine wichtige Option dar, um auf zukünftige Veränderungen des Kommunikationsverhaltens von Störern der öffentlichen Sicherheit reagieren zu können. Dabei würde der Einsatz dieses Instrumentariums teilweise sogar zu einer geringeren Eingriffsintensität im Vergleich zur Abwehr derselben Gefahrenlage durch andere Maßnahmen führen.

Gleichwohl hat die verfassungsrechtliche Bewertung – u.a. vor dem Hintergrund der Entscheidung des BVerfG zu verschiedenen Normen des BKAG[816] – und die Auswertung der empirisch erhobenen Daten Hinweise auf einige wenige sinnvolle Klarstellungs- und notwendige Änderungsbedarfe ergeben.

Als problematisch zu beurteilen ist etwa die Zuständigkeit des OVG für die im Rahmen des Richtervorbehalts vorzunehmenden Maßnahmen. Zwar lässt sich die Zulässigkeit der gesetzlichen Bestimmung der Zuständigkeit eines Gerichts des Verwaltungsrechtswegs daraus herleiten, dass die Zulässigkeit des Verwaltungsrechtswegs bereits nach der allgemeinen Norm des § 40 Abs. 1 VwGO gegeben ist. Anders zu beurteilen ist jedoch die Zuweisung der sachlichen Zuständigkeit an das OVG. Hier gilt der Grundsatz des § 45 VwGO – Zuständigkeit der Verwaltungsgerichte im ersten Rechtszug –, da der Landesgesetzgeber mangels Öffnungsklausel nicht befugt ist, eine hiervon abweichende Re-

816 BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09 und 1 BvR 1140/09.

gelung zu treffen. Da auch eine Zuweisung an den VerfGH Rh-Pf. ausscheidet,[817] verbleiben als Möglichkeiten lediglich die Zuweisung an die ordentliche Gerichtsbarkeit oder die Verwaltungsgerichte.

Dabei sollte darauf geachtet werden, eine einheitliche Gerichtszuständigkeit für die POG-Maßnahmen zu schaffen. Im Falle einer Änderung der Zuständigkeitszuweisung müsste der Gesetzgeber entscheiden, welchen Kriterien er größeres Gewicht beimisst: der Frage der Fachkompetenz, dem Aspekt der Ortsnähe oder der Möglichkeit, Routinen auszubilden und somit auch Kompetenzen aufzubauen. Während die Fachkompetenz für die Anwendung des Polizeirechts bei den Verwaltungsgerichten liegt, wäre unter dem Aspekt der Ortsnähe eine Zuweisung an die Amtsgerichte zu bevorzugen. Bei der ordentlichen Gerichtsbarkeit kommt hinzu, dass sowohl Amts- als auch Landgerichte bereits für einschlägige Entscheidungen im Rahmen der StPO zuständig sind, so dass hier bereits vergleichbares Erfahrungswissen vorhanden ist und durch die zu erwartende höhere Fallzahl von Entscheidungen auch voraussichtlich vertieft werden kann. Durch die Zuweisung an die Verwaltungsgerichte wiederum könnte eine Rechtswegspaltung vermieden werden.

Das Zusammenspiel zwischen den den § 29 Abs. 5 POG für entsprechend anwendbar erklärenden §§ 31 Abs. 7, § 31b Abs. 4, § 31c Abs. 6 und § 31e Abs. 2 POG und der in Bezug genommenen Norm ist für die Praxis nur schwer zu handhaben. Daher sollte durch eine entsprechende Gesetzesänderung klargestellt werden, dass die „entsprechende Anwendung“ des § 29 Abs. 5 POG nicht dazu führt, dass zusätzlich die Anforderungen der StPO an die Rechtfertigung einer Wohnraumüberwachung erfüllt sein müssen, sondern dass immer nur die Anforderungen der StPO an die Rechtfertigung der *jeweiligen*, nach dem POG ergriffenen Maßnahme vorliegen müssen.

Das BVerfG hat eine aufsichtliche Kontrolle der verdeckten Überwachungsmaßnahmen angemahnt, was u.a. eine unabhängige Sichtung der erhobenen Daten, eine turnusmäßige Kontrolle durch eine mit wirksamen Befugnissen ausgestattete Stelle und Berichtspflichten gegenüber Parlament und Öffentlichkeit einschließt.

---

817 Auch wenn die Nutzung der beim VerfGH vorhandenen „profunden Kenntnisse des Verfassungs- und Verwaltungsrechts“, ein legitimes Anliegen darstellen, handelt es sich doch nicht um eine verfassungsrechtliche Streitigkeit; vgl. hierzu *Held*, in: Grimm/ Caesar, Verf Rh-Pf, Art. 135 Rn. 5.

5.2 § 29 POG

Die Datenerhebung durch den verdeckten Einsatz technischer Mittel in oder aus Wohnungen gemäß § 29 POG ist im Evaluationszeitraum nicht zum Einsatz gekommen – wohl weil die Vorbereitung und Durchführung mit einem erheblichen personellen, zeitlichen und technischen Aufwand verbunden ist. Daher werden zunächst einmal alle anderen zur Verfügung stehenden Möglichkeiten ausgeschöpft, bevor eine Wohnraumüberwachung in Betracht gezogen wird. Dennoch ist die gesetzliche Zurverfügungstellung der Maßnahme als sinnvoll zu erachten, um besonderen Gefährdungslagen Rechnung tragen zu können. Verfassungsrechtlich bedenklich ist im Rahmen des § 29 Abs. 1 POG die Möglichkeit, Maßnahmen gegen Kontakt- und Begleitpersonen sowie Nichtstörer zu adressieren. Der Verweis auf einen Straftatenkatalog ist dagegen als verfassungskonform zu bewerten. Vorbereitungs- und Begleitmaßnahmen zur Anbringung der technischen Mittel sowie die technische Durchführung sind als Annexkompetenz von der Maßnahme umfasst.

Eine Herausforderung im Zusammenhang mit der Wohnraumüberwachung stellt für die Polizei die Gewährleistung des Kernbereichsschutzes dar. So ist nicht immer klar, wann eine Berührung des Kernbereichs erfolgt und wann die Überwachung wieder fortgesetzt werden kann, wenn eine Berührung des Kernbereichs zuvor festgestellt wurde. Hier könnte die Schaffung der rechtlichen Möglichkeit, den Kernbereichsschutz durch die partielle Löschung einer gefertigten Aufzeichnung zu gewährleisten, in Betracht gezogen werden, durch die ggf. nicht nur die Effektivität der polizeilichen Arbeit, sondern auch der Grundrechtsschutz verbessert werden könnte. Dabei wäre allerdings darauf zu achten, dass der Zweistufigkeit des Kernbereichsschutzes hinreichend Rechnung getragen wird.

5.3 § 31 POG

5.3.1 TKÜ nach § 31 Abs. 1, 2 POG

Die TKÜ nach § 31 Abs.1, 2 POG ist bislang am häufigsten zur Anwendung gekommen, wenngleich auch nur drei der sechs rheinland-pfälzischen Polizeibehörden im Evaluationszeitraum nennenswerte Erfahrungen mit dieser Maßnahme sammeln konnten: Gerade einmal eine Maßnahme alle zwei Monate sind im Evaluationszeitraum durchgeführt worden. In der Hälfte der Fälle haben die Polizeibehörden zunächst versucht die Daten auf anderem Wege zu

erheben, bevor eine TKÜ beantragt wurde. Dies deutet auf einen maßvollen und verantwortungsvollen Umgang der Polizei mit dem Instrument der präventiven Telekommunikationsüberwachung hin. Zudem zeichnet sich die Maßnahme durch einen hohen Nutzen für die polizeiliche Arbeit aus.

Lässt man zwei Extremfälle im Polizeipräsidium Mainz unberücksichtigt, wird deutlich, dass sich die Maßnahmen im Durchschnitt gegen eine Person (v.a. Verhaltensstörer) gerichtet haben. Der Schwerpunkt bei der Anwendung des § 31 Abs. 1 POG liegt auf der verdeckten Erhebung von Verkehrsdaten, während Gesprächsinhalte seltener überwacht werden. In keinem Fall wurde die maximal mögliche Befristungsdauer ausgeschöpft. Der Großteil der Maßnahmen wird auf nicht länger als fünf Wochen befristet. Auch die tatsächliche Dauer der Datenerhebung beträgt im Großteil der Fälle nicht länger als 31 Tage, so dass Verlängerungsanträge bislang nicht gestellt wurden. Dass die Polizeibehörden sehr bedacht im Umgang mit der Maßnahme sind, zeigt sich auch daran, dass sie bislang nur in zwölf Fällen auf ihre Eilkompetenz bei Gefahr in Verzug zurückgegriffen haben.

Hinsichtlich der Wirksamkeit der durchgeführten Maßnahmen ist festzustellen, dass diese im Großteil der Fälle zu einer Erhärtung eines Gefahren- bzw. Straftatenverdachts beigetragen haben. Noch deutlicher zeigt sich die Wirksamkeit anhand der Bewertung des Nutzens der im Rahmen der Maßnahme gewonnenen Daten durch die Polizeibehörden. Diese wird im Großteil der Fälle als hoch bzw. sehr hoch eingestuft. Mit Blick auf die Erhöhung der Eingriffsintensität durch die parallele Durchführung von Datenerhebungsmaßnahmen zeigt sich, dass immerhin in über der Hälfte der Fälle darauf verzichtet wurde.

Die Vorschrift begegnet unter dem Aspekt der Normenbestimmtheit keinen Bedenken. Die Aufnahme von Nichtstören in den Adressatenkreis der Norm ist allerdings nicht frei von verfassungsrechtlicher Kritik.

5.3.2 Quellen-TKÜ nach § 31 Abs. 3 POG

Durch die Normierung der Quellen-TKÜ hat der Gesetzgeber auf die technologische Entwicklung und das veränderte Kommunikationsverhalten reagiert. Ohne diese Regelung wird es in Zukunft kaum noch möglich sein, bestimmte Daten zu erheben, da die Kommunikation heute mittlerweile häufig verschlüsselt stattfindet.

Die Maßnahme ist nach dem derzeitigen technischen Stand praktisch nicht anwendbar. Es kann technisch nicht sichergestellt werden, dass ausschließlich

laufende Telekommunikation betroffen ist. Weder dies noch andere Gesichtspunkte führen jedoch zu Zweifeln an der Verfassungsgemäßheit der Norm.

5.3.3 Mitwirkung der Diensteanbieter nach § 31 Abs. 6 POG

§ 31 Abs. 6 POG begegnet keinen grundsätzlichen Bedenken. Es ist allerdings darauf hinzuweisen, dass die Vorschrift die TK-Diensteanbieter ausschließlich zur Übermittlung von Verkehrsdaten verpflichtet, nicht jedoch zur Übermittlung von Bestandsdaten. Da eine Bestandsdatenabfrage nach der Judikatur des BVerfG nicht mehr auf die Generalklausel des § 26 POG gestützt werden kann, ist es in Rheinland-Pfalz aktuell nicht möglich, Bestandsdaten bei den Diensteanbietern zu erheben.

Auch wenn es bislang nur wenige Probleme bei der Zusammenarbeit zwischen Providern und Polizeibehörden gibt – lediglich bei sechs Maßnahmen wird auf solche hingewiesen –, könnte erwogen werden, ob es nicht u.U. sinnvoll ist, gesetzlich zu regeln, dass die Diensteanbieter dazu verpflichtet werden, die erforderlichen Daten unverzüglich und in einem einheitlichen Format zur Verfügung zu stellen, um die Arbeit der Polizeibehörden zu erleichtern.

5.4 § 31b POG

§ 31b POG bezieht sich ausschließlich auf reine Telemediendiensteanbieter. Ermöglicht wird ausschließlich der Zugriff auf Nutzungsdaten, die das Pendant zu Verkehrsdaten im Bereich des TKG darstellen. In der Praxis ist diese Regelung erst einmal zur Anwendung gekommen. Dennoch ist die Normierung der Maßnahme positiv zu bewerten, da der Gesetzgeber auf die technologische Entwicklung reagiert und die Möglichkeit geschaffen hat, diese Daten verdeckt zu erheben.

Ähnlich wie im Bereich des TKG kommt eine Abfrage von Bestandsdaten mangels spezieller gesetzlicher Grundlage derzeit in Rheinland-Pfalz nicht in Betracht. Auffällig ist bei § 31b POG, dass hier durch den Verzicht auf das Vorliegen einer gegenwärtigen Gefahr eine niedrigere Eingriffsschwelle als bei § 31 POG normiert wurde. Auch wenn diese niedrigere Eingriffsschwelle unter verfassungsrechtlichen Aspekten nicht zu beanstanden ist, scheint sie angesichts der Nähe der Maßnahme zur Verkehrsdatenerhebung nach § 31 POG doch rechtfertigungsbedürftig und eine entsprechende gesetzgeberische Überprüfung wäre wünschenswert.

5.5 § 31c POG

Eine Online-Durchsuchung ist bisher von den Polizeibehörden in Rheinland-Pfalz nicht durchgeführt worden. Dies hängt insbesondere mit den bereits im Zusammengang mit der Quellen-TKÜ geschilderten technischen und verfassungsrechtlichen Anforderungen zusammen. So sind auch hier die rechtlichen Voraussetzungen geschaffen worden, um auf die technologische Entwicklung reagieren zu können. Aufgrund des Fehlens einer entsprechenden Software ist die Maßnahme allerdings technisch derzeit nicht umsetzbar. Zudem ist die Durchführung der Maßnahme mit einem großen personellen und technischen Aufwand verbunden.

Absatz 1 könnte um die Wörter „bestimmte Tatsachen“ ergänzt werden, um eine über jeden Zweifel erhabene Normenbestimmtheit zu erzielen. Die Entscheidungen des BVerfG zu dieser Frage sind nicht eindeutig, sprechen aber für dieses Verständnis. Die Möglichkeit, gemäß § 31 Abs. 1 S. 1 Nr. 2 POG Online-Durchsuchungen gegenüber Nachrichtenmittlern durchzuführen, ist verfassungsrechtlich bedenklich. Vorfeldmaßnahmen nach § 31c Abs. 3 sind zwar zulässig, ein Betretungsrecht der Wohnung, um die Vorrichtungen anzubringen, lässt sich aus der Vorschrift aber nicht herleiten. Das Fehlen dieses Rechts führt dennoch nicht zur Ungeeignetheit der Maßnahme, da die Durchführung der Online-Durchsuchung auch anderweitig sichergestellt werden kann.

5.6 § 31e POG

Bislang ist die Funkzellenabfrage gemäß § 31e POG in Rheinland-Pfalz nicht zum Einsatz gekommen. Somit liegen keine Erfahrungswerte im Umgang mit der Maßnahme vor. Dennoch kann es als sinnvoll angesehen werden, dass analog zur StPO auch eine Ermächtigungsgrundlage im POG zur Durchführung einer Funkzellenabfrage geschaffen wurde. Die bei der Funkzellenabfrage durchzuführende Auswertung von Massendaten ist sehr komplex und aufwändig. Daher ist davon auszugehen, dass die Maßnahme auch in Zukunft nur selten zum Einsatz kommen wird.

Mit Blick auf die Normenklarheit sollte der Gesetzgeber prüfen, ob sich der Gesetzeswortlaut nicht ausdrücklich zu der Frage verhalten sollte, ob die Ermächtigung Auskünfte über bereits angefallene oder zukünftig erst anfallende Verkehrsdaten oder beides umfasst. Entsprechendes gilt für eine Regelung der

Frage, gegen wen sich die Maßnahme richten darf. In die Prüfung eines bestehenden Änderungsbedarfs sollte auch einbezogen werden,

- ob die Inbezugnahme in § 39a Abs. 3 bis 5 POG nicht auf § 31e erweitert wird, da schwer zu erkennen ist, warum § 31e POG im Hinblick auf den Kernbereichsschutz nicht ebenso behandelt wird wie § 31 POG oder wie der im Bereich der Telemedien vergleichbare § 31b POG;
- ob nicht eine Vereinheitlichung der Bedingungen für die Datenanlieferung durch den Provider als notwendig zu erachten ist.

5.7 § 38 POG

Die Regelung zur präventiven Rasterfahndung trägt den diesbezüglichen Vorgaben des BVerfG Rechnung und begegnet daher keinen grundsätzlichen Bedenken. Im Evaluationszeitraum haben die Polizeibehörden noch keine Erfahrungen mit der neugefassten Regelung sammeln können. Dennoch wird die gesetzliche Zurverfügungstellung von den Polizeibehörden positiv bewertet. Allein die Auswertung von Massendaten wird als sehr aufwändig und schwierig angesehen. Es ist davon auszugehen, dass die präventive Rasterfahndung in Zukunft nur in ganz seltenen Fällen zum Einsatz kommen wird.

5.8 § 39a POG

§ 39a Abs. 1 und 5 POG sind ebenso verfassungskonform wie § 39a Abs. 2 i.V.m. § 29 POG. § 39a Abs. 3 i.V.m. §§ 31, 31b, 31c POG wurde von der wissenschaftlichen Literatur bislang für verfassungswidrig gehalten. In Anlehnung an die Entscheidung des BVerfG zu § 100a Abs. 4 StPO entspricht die Norm allerdings den verfassungsrechtlichen Vorgaben. Der Gesetzgeber hat aber die technische Entwicklung zu beobachten.

§ 39a Abs. 4 POG ist nicht verfassungskonform. Die Regelungen zur Prüfung einer Kernbereichsrelevanz von Daten, die im Rahmen von Wohnraumüberwachungen (§ 29 POG) oder Online-Durchsuchungen (§ 31c POG) erhoben wurden, genügen nicht den verfassungsrechtlichen Anforderungen. Die Durchsicht muss durch eine unabhängige Stelle erfolgen, was durch die jetzige Konstellation nicht gewährleistet ist, und bereits vor einer Auswertung durch die Polizeibehörde als Filter dienen.

5.9 § 39b POG

Der Schutz von Berufsgeheimnisträgern nach § 39b POG steht im Spannungsverhältnis zwischen dem Schutz der Menschenwürde und dem Gebot effektiver Gefahrenabwehr und Strafverfolgung. Aus diesem Grund ist ein absoluter Schutz von Berufsgeheimnisträgern nur in Ausnahmefällen zulässig. Der Schutz des § 39b Abs. 1 POG geht darüber hinaus und sollte durch eine Abwägungsklausel geöffnet werden.

5.10 § 40 Abs. 5, 6 POG

Erkenntnisse im Bereich der Unterrichtungsvorschriften der Absätze 5 und 6 des § 40 POG konnten bislang nur im Zusammenhang mit Maßnahmen gemäß § 31 Abs. 1 POG gewonnen werden. Hier zeigt sich, dass in knapp der Hälfte der Fälle keine Unterrichtung der Personen erfolgte, gegen die sich die Maßnahmen gerichtet haben. Als Hauptgründe hierfür wurden die unverzügliche Vernichtung der personenbezogenen Daten sowie der Anschluss eines strafrechtlichen Verfahrens genannt. In den übrigen 18 Fällen erfolgte die Unterrichtung der Personen, gegen die sich die Maßnahmen gerichtet haben, in der Regel sehr schnell.

§ 40 Abs. 5 POG entspricht größtenteils den Vorgaben des BVerfG. Problematisch ist alleine Satz 2 der Norm: Er gestaltet die Benachrichtigungspflicht einerseits zu streng aus, andererseits ist er nicht weitreichend genug. Auf der einen Seite fehlt eine Abwägungsmöglichkeit, die auch bei den in Satz 2 besonders erwähnten Betroffenen ein Absehen von der Benachrichtigung im Einzelfall zulässt. Auf der anderen Seite fehlt die Normierung einer grundsätzlichen Benachrichtigungspflicht auch gegenüber „nur“ einfach Betroffenen, die weder Objekt einer Maßnahme nach §§ 29, 31c POG geworden sind noch besonders schutzwürdige Interessen an der Benachrichtigung geltend machen können. Insofern wäre eine gesetzgeberische Korrektur anzuraten.

§ 40 Abs. 6 POG normiert Ausnahmen von der Benachrichtigungspflicht nach § 40 Abs. 5 POG, die – bei entsprechender Auslegung – verfassungsrechtlich nicht zu beanstanden sind.

Literaturverzeichnis

Abate, Constantin, Onlinedurchsuchung, Quellen-Telekommunikationsüberwachung und die Tücke im Detail, in: DuD 2011, S. 122 ff.

Abel, Ralf B., Der behördliche Datenschutzbeauftragte, in: MMR 2002, S. 289 ff.

Achelpöhler, Wilhelm/ Niehaus, Holger, Rasterfahndung als Mittel zur Verhinderung von Anschlägen islamistischer Terroristen in Deutschland, in: DÖV 2003, S. 49 ff.

Aernecke, Eva, Der Schutz elektronischer Daten im Verfassungsrecht, Dissertation, 2012 (zit.: Aernecke, Schutz).

Albrecht, Florian/ Dienst, Sebastian, Der verdeckte hoheitliche Zugriff auf informationstechnische Systeme – Rechtsfragen von Onlinedurchsuchung und Quellen-TKÜ, in: JurPC, Web-Dok. 5/2012, Abs. 1 – 65, abrufbar unter: http://www.jurpc.de/jurpc/show?id=20120005

Aschmann, Tjark Erich, Der Richtervorbehalt im deutschen Polizeirecht, Dissertation, 1999.

Bader, Johann/ Funke-Kaiser, Michael/ Stuhlfauth, Thomas/ v. Albedyll, Jörg (Hrsg.), Verwaltungsgerichtsordnung, 6. Aufl. 2015 (zit.: Bearbeiter, in: Bader u.a., VwGO).

Bäcker, Matthias, Terrorismusabwehr durch das Bundeskriminalamt, 2009 (zit.: Bäcker, BKA).

Bäcker, Matthias, Das IT-Grundrecht: Funktion, Schutzgehalt, Auswirkungen auf staatliche Ermittlungen, in: Uerpmann-Wittzack, Robert (Hrsg): Das neue Computergrundrecht, S. 1 ff. (zit.: Bäcker, IT-Grundrecht).

Bär, Wolfgang, Telekommunikationsüberwachung und andere verdeckte Ermittlungsmaßnahmen – Gesetzliche Neuregelungen zum 1.1.2008, in: MMR 2008, S. 215 ff.

Baum, Gerhart Rudolf/ Schantz, Peter, Die Novelle des BKA-Gesetzes – Eine rechtspolitische und verfassungsrechtliche Kritik, in: ZRP 2008, 137 ff.

Bausback, Winfried, Fesseln für die wehrhafte Demokratie?, in: NJW 2006, S. 1922 ff.

Beckmann, Klaus/ Schröder, Bernhard, PdK, Polizei- und Ordnungsbehördengesetz, Band 30, 2008-2013 (zit.: Beckmann/ Schröder, PdK).

Berger, Ernst Georg, Wer anschaffen will, muss auch zahlen, in: CR 2008, S. 557 ff.

Berlit, Uwe, Richtervorbehalte: Gerichtliche Verwaltungstätigkeit oder Rechtsprechung? Zur Vereinbarkeit des Richtervorbehalts bei der präventivpolizeilichen Kontrollstelle nach § 14 NGefAG mit § 39 VwGO, in: NdsVBl 1995, S. 197 ff.

Berner, Georg/ Köhler, Michael/ Käß, Robert, Polizeiaufgabengesetz, 20. Aufl. 2010 (zit.: Berner/ Köhler/ Käß, BayPAG).

Bode, Thomas, Bestandsdatenauskunft im Brandenburgischen Polizeigesetz - Keine konkrete Gefahr, aber eingeschränkte Rechtsgüter?, in: NJ 2005, 5 ff.

Böckenförde, Thomas, Auf dem Weg zur elektronischen Privatsphäre, in: JZ 2008, S. 925 ff.

Böhrenz, Gunter/ Siefken, Peter, Niedersächsisches Gesetz über die öffentliche Sicherheit und Ordnung, 9. Aufl. 2014 (zit.: Böhrenz/ Siefken, Nds. SOG).

Bonin, Irina, Grundrechtsschutz durch verfahrensrechtliche Kompensation bei Maßnahmen der polizeilichen Informationsvorsorge, Dissertation, 2010 (zit.: Bonin, Grundrechtsschutz).

Bratke, Bastian, Die Quellen-Telekommunikationsüberwachung im Strafverfahren, Dissertation, 2013 (zit.: Bratke, Quellen-TKÜ).

Braun, Frank/ Roggenkamp, Jan Dirk, Ozapftis – (Un)Zulässigkeit von „Staatstrojanern“, in: K&R 2011, S. 681 ff.

Buchholtz, Gabriele, Kein Sonderopfer für die Sicherheit – BVerfG erklärt für BKAG für verfassungswidrig, NVwZ 2016, S. 906 ff.

Buermeyer, Ulf, Zum Begriff der »laufenden Kommunikation« bei der Quellen-Telekommunikationsüberwachung (»Quellen-TKÜ«), in: StV 2013, S. 470 ff.

Buermeyer, Ulf, Verfassungsrechtliche Grenzen der „Onlinedurchsuchung“, in: RDV 2008, S. 8 ff.

Buermeyer, Ulf/ Bäcker, Matthias, Zur Rechtswidrigkeit der Quellen-Telekommunikationsüberwachung auf Grundlage des § 100a StPO, in: HRRS 2009, S. 433 ff.

Chadoian, Satenig M., Das Fernmeldegeheimnis im Zeitalter der Internet- und Mobilfunküberwachung, 2015 (zitiert: Chadoian, Das Fernmeldegeheimnis im Zeitalter der Internet- und Mobilfunküberwachung).

Coen, Christoph, Zählt ein Handy für die Überwachungskosten als DSL-Anschluss?, in: CR 2013, S. 217 ff.

Darnstädt, Thomas, Karlsruher Gefahr - Eine kritische Rekonstruktion der polizeirechtlichen Ausführungen des Bundesverfassungsgerichts im Vorratsdaten-Urteil und im Online-Urteil, in: DVBl. 2011, S. 263 ff.

Deutscher Juristentag, 69. Deutscher Juristentag, München, 2012, http://www.djt.de/fileadmin/downloads/69/121206_djt_69_beschluesse_web_rz.pdf.

Drallé, Lutz, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, Dissertation, 2010 (zit.: Drallé, Vertraulichkeit).

Dreier, Horst (Hrsg.), Grundgesetz Kommentar, Band I: Präambel, Artikel 1-19, 3. Aufl. 2013 (zit.: Bearbeiter, in: Dreier, GG, Band I).

Durner, Wolfgang, Anmerkung zu BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09 – Verfassungswidrigkeit einzelner Ermittlungsbefugnisse des BKA zur Terrorismusbekämpfung, in: DVBl. 2016, S. 770 ff.

Ebert, Frank/ Seel, Lothar, Thüringer Gesetz über die Aufgaben und Befugnisse der Polizei, 6. Aufl. 2012 (zit.: Ebert/ Seel, ThürPAG).

Eckhardt, Jens, Anmerkung zum Beschluss des BVerfG vom 13.11.2010 (2 BvR 1124/10 K&R 2011, 320), in: KuR 2011, S. 323 ff.

Ehlers, Dirk/ Fehling, Michael/ Pünder, Hermann (Hrsg.), Besonderes Verwaltungsrecht, Band 3, 3. Aufl. 2013 (zit.: Bearbeiter, in: Ehlers/ Fehling/ Pünder, Verwaltungsrecht 3).

Eisenberg, Ulrich, Beweisrecht der StPO, Spezialkommentar, 9. Aufl. 2015 (zit.: Eisenberg, StPO).

Ende, Claudia, Verstärkter Schutz von Berufsgeheimnisträgern – auch für Steuerberater!, in: DStR 2009, S. 2556 ff.

Epping, Volker/ Hillgruber, Christian (Hrsg.), GG, Stand 01.03.2016 (zit.: Bearbeiter, in: Epping/ Hillgruber, GG).

Fehling, Michael/ Kastner, Berthold/ Störmer, Rainer (Hrsg.), Verwaltungsrecht, Handkommentar, 4. Aufl. 2016 (zit.: Bearbeiter, in: Hk-VerwR).

Gärditz, Klaus F. (Hrsg.), Verwaltungsgerichtsordnung (VwGO) mit Nebengesetzen, 2013 (zit.: Bearbeiter, in: Gärditz, VwGO).

Generalbundesanwalt *beim Bundesgerichtshof,* Rechtliche Zulässigkeit der sog. „Quellen-TKÜ“, in: StV 2013, S. 476 ff.

Gercke, Björn/ Julius, Klaus- Peter/, Temming, Dieter/ Zöller, Mark (Hrsg.), Strafprozessordnung, 2011 (zit.: Bearbeiter, in: Gercke u.a., StPO).

Globig, Klaus/Schuber, Norbert/ Hartig, Judith/ Klink, Judith/Eiermann, Helmut (Hrsg.), Landesdatenschutzgesetz Rheinland-Pfalz, Praxis der Kommunalverwaltung Band 16, 2009 (zit.: Globig u.a., LDSG).

Graf, Jürgen Peter (Hrsg.), Strafprozessordnung, Beck´scher Online-Kommentar StPO, Stand: 25. Ed. 2016 (zit.: Bearbeiter, in: Graf, StPO).

Grimm, Christoph/ Caesar, Peter (Hrsg.), Verfassung für Rheinland-Pfalz, Kommentar, 2001 (zit.: Bearbeiter, in: Grimm/ Caesar, Verf Rh-Pf).

Guckelberger, Annette/ Hero, Kristin, Das Gesetz zur Erhöhung der inneren Sicherheit im Saarland, in: LKRZ 2008, S. 161 ff.

Gudermann, Anne, Onlinedurchsuchung im Lichte des Verfassungsrechts, Dissertation, 2010 (zit.: Gudermann, Onlinedurchsuchung).

Gusy, Christoph, Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, in: DuD 2009, S. 33 ff.

Haas, Günter, Der „Große Lauschangriff" - klein geschrieben -, in: NJW 2004, S. 3082 ff.

Hannich, Rolf (Hsrg.), Karlsruher Kommentar zur Strafprozessordnung, 7. Aufl. 2013 (zit.: Bearbeiter, in: KK-StPO).

Hendler, Reinhard/ Hufen, Friedhelm/ Jutzi, Siegfried (Hrsg.), Landesrecht Rheinland-Pfalz, 7. Aufl. 2014 (zit.: Bearbeiter, in: Landesrecht Rh-Pf).

Henrichs, Axel, Zur rechtlichen Zulässigkeit der Quellen-TKÜ, in: Kriminalistik 2008, S. 438 ff.

Hoffmann, Christian, Die Gewährleistung der Vertraulichkeit und Integrität elektronischer Daten- und Dokumentensafes, Dissertation, 2012 (zit.: Hoffmann, Vertraulichkeit).

Hoffmann-Riem, Wolfgang, Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, in: JZ 2008, S. 1009ff.

Honnacker, Heinz/ Beinhofer, Paul/ Hauser, Manfred (Hrsg.), Polizeiaufgabengesetz - PAG - Gesetz über die Aufgaben und Befugnisse der Bayerischen Staatlichen Polizei, 20. Aufl. 2014 (zit.: Bearbeiter, in: Honnacker, u.a., PAG)

Horn, Hans-Detlef, Vorbeugende Rasterfahndung und informationelle Selbstbestimmung, in: DÖV 2003, S. 746 ff.

Hornmann, Gerhard, Hessisches Gesetz über die öffentliche Sicherheit und Ordnung (HSOG), Kommentar, 2. Aufl. 2008 (zit.: Hornmann, HSOG).

Hornung, Gerrit, Ermächtigungsgrundlage für die „Onlinedurchsuchung“?, in: DuD 2007, S. 575 ff.

Hsieh, Shuo-Chun, E-Mail-Überwachung zur Gefahrenabwehr, Dissertation, 2011 (zit.: Hsieh, E-Mail-Überwachung).

Jarass, Hans D./ Pieroth, Bodo, Grundgesetz für die Bundesrepublik Deutschland, Kommentar, 14. Aufl. 2016 (zit.: Bearbeiter, in: Jarass/ Pieroth, GG).

Käß, Robert, Die Befugnis zum verdeckten Zugriff auf informationstechnische Systeme im bayerischen Polizeiaufgabengesetz (sog. Online-Überwachung oder Online-Durchsuchung), in: BayVBl 2010, S. 1 ff.

Käß, Robert, Die Änderung der Rasterfahndung im Bayerischen Polizeiaufgabengesetz (PAG), in: BayVBl. 2009, S. 360 ff.

Kalina-Kerschbaum, Claudia, Anmerkung zu BVerfG, Beschluss vom 12. 10. 2011 - 2 BvR 236/08, 2 BvR 237/08, 2 BvR 422/08, in: DStR 2012, S. 537 ff.

Kilian, Wolfgang/ Heussen, Benno (Hrsg.), Computerrechts-Handbuch, Informationstechnologie in der Rechts- und Wirtschaftspraxis, Teil 13: Datenschutz, Stand August 2013 (zit.: Bearbeiter in: Kilian/ Heussen, Handbuch, Teil 13).

Kirchhof, Gregor, Kumulative Belastung durch unterschiedliche staatliche Maßnahmen, in: NJW 2006, S. 732 ff.

Knauer, Wolfgang/ Kudlich, Klaus/ Schneider, Hartmut (Hrsg.), Münchener Kommentar zur StPO, Band 1, 2014 (zitiert: Bearbeiter, in: MüKo StPO).

Kniesel, Michael, Zur Frage der Eignung der Rasterfahndung zur Gefahrenabwehr sowie der Beschwerdeberechtigung der antragstellenden Behörde, in: NJ 2003, S. 37 ff.

Köhler, Sebastian, Zu den Alternativen des Rechtsschutzes gegen die richterliche Bestätigung von Eingriffen in Telekommunikationsvorgänge, in: JR 2006, S. 287 ff.

Kötter, Matthias, Novellierung der präventiven Wohnraumüberwachung?, in: DÖV 2005, S. 225 ff.

Kopp, Ferdinand O./ Schenke, Wolf-Rüdiger, Verwaltungsgerichtsordnung, Kommentar, 22. Aufl. 2016 (zit.: Kopp/ Schenke, VwGO)

Kube, Hanno/ Schütze, Marc, Die Kosten der TK-Überwachung, in: CR 2003, S. 663 ff.

Von Kühlewein, Malte Rabe, Der Richtervorbehalt im Polizei- und Strafprozeßrecht, Dissertation, 2001 (zit.: von Kühlewein, Richtervorbehalt).

Kugele, Dieter, VwGO – Verwaltungsgerichtsordnung, Kommentar, 2013.

Kugelmann, Dieter, BKA-Gesetz, 2014 (zit.: Kugelmann, BKA-Gesetz).

Kulwicki, Christine, Verfassungswandel. Die Wechselwirkung zwischen Grundrechten und informationstechnischen Ermittlungsmethoden, Dissertation, 2012 (zit.: Kulwicki, Verfassungswandel).

Kutscha, Martin, Das „Computergrundrecht" – eine Erfolgsgeschichte?, in: DuD 2012, S. 391 ff.

Kutscha, Martin, Verdeckte „Onlinedurchsuchung" und Unverletzlichkeit der Wohnung, in: NJW 2007, S. 1169 ff.

Leipold, Klaus, Verfassungsmäßigkeit heimlicher Datenerhebungen nach Polizeirecht, in: NJW-Spezial 2013, S. 56 ff.

Lisken, Hans/ Denninger, Erhard (Hrsg.), Handbuch des Polizeirechts, 5. Aufl. 2012 (zit.: Bearbeiter, in: Lisken/ Denninger, Handbuch).

Lisken, Hans, Zur polizeilichen Rasterfahndung, in: NVwZ 2002, S. 513 ff.

Löffelmann, Markus, Aktuelle Rechtsprobleme der Telekommunikationsüberwachung, in: AnwBl 2006, S. 598 ff.

Luch, Anika D., Der Einsatz des „Staatstrojaners" – Zusammenspiel von effektiver Gesetzgebung, Rechtswirklichkeit und Exekutivkontrolle, in: BRJ 2012, S. 34 ff.

Lücke, Gerhard, Grundsätze des Verwaltungsprozesses, in: JuS 1961, S. 41 ff.

Lüdemann, Jörn, Richtervorbehalte in der Verwaltungsgerichtsbarkeit?, in: DÖV 1996, S. 870 ff.

Von Mangoldt, Hermann/ Klein, Friedrich/ Starck (Hrsg.), Christian, Kommentar zum Grundgesetz, Band 2: Artikel 20 bis 82, 6. Aufl. 2010 (zit.: Bearbeiter in: v. Mangoldt/ Klein/ Starck, GG, Band 2).

Maunz, Theodor, Dürig, Günter (Hrsg.), Grundgesetz Kommentar, Stand: 76. Ergänzungslieferung Dezember 2015 (zit.: Bearbeiter, in: Maunz/ Dürig, GG).

Meixner, Kurt/ Fredrich, Dirk, Hessisches Gesetz über die öffentliche Sicherheit und Ordnung HSOG, 112. Aufl. 2016 (zit.: Meixner/ Fredrich, HSOG).

Merten, Detlef/ Papier, Hans-Jürgen (Hrsg.), Handbuch der Grundrechte, Band IV, 2011 (zit.: Bearbeiter, in: HdbGR, Band IV).

Meyer-Goßner, Lutz/ Schmitt, Bertram (Hrsg.), Strafprozessordnung, 59. Aufl. 2016 (zit.: Bearbeiter, in: Meyer-Goßner/ Schmitt, StPO).

Möstl, Markus, Das Bundesverfassungsgericht und das Polizeirecht. Eine Zwischenbilanz aus Anlass des Urteils zur Vorratsdatenspeicherung, in: DVBl. 2010, S. 808 ff.

Möstl, Markus, Die neue dogmatische Gestalt des Polizeirechts in: DVBl. 2007, S. 581 ff.

Petri, Thomas, Bayerischer Landesbeauftragter für Datenschutz, Prüfbericht Quellen-TKÜ vom 30.07.2012, (zit.: Petri, Prüfbericht), abrufbar unter: http://www.datenschutz-bayern.de/0/bericht-qtkue.pdf.

Pieroth, Bodo/ Schlink, Bernhard/ Kniesel, Michael, Polizei- und Ordnungsrecht, 8. Aufl. 2014 (zit.: Pieroth/ Schlink/ Kniesel, POR).

Poscher, Ralf, Menschenwürde und Kernbereichsschutz. Von den Gefahren einer Verräumlichung des Grundrechtsdenkens, in: JZ 2009, S. 269 ff.

Posser, Herbert/ Wolff, Heinrich Amadeus (Hrsg.), Beck'scher Online-Kommentar VwGO, Stand: 37. Edition 2016 (zit.: Bearbeiter, in: Posser/ Wolff, VwGO).

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

Rauscher, Thomas/ Wax, Peter/ Wenzel, Joachim, Münchener Kommentar zur Zivilprozessordnung mit Gerichtsverfassungsgesetz und Nebengesetzen (Hrsg.), Band 1, 4. Aufl. 2013 (zit.: Bearbeiter, in: MüKo ZPO).

Ritter, Markus, Vorratsdatenspeicherung, Telekommunikationsüberwachung und (sonstige) heimliche Ermittlungsmaßnahmen der StPO, Dissertation, 2011 (zit.: Ritter, Vorratsdatenspeicherung).

Robrecht, Michael P., Die präventive Rasterfahndung im Lichte der aktuellen Verfassungsrechtsprechung, in: SächsVBl. 2007, S. 80 ff.

Roggan, Fredrik, Das neue BKA-Gesetz – Zur weiteren Zentralisierung der deutschen Sicherheitsarchitektur -, in: NJW 2009, S. 257 ff.

Roggan, Fredrik, Der tkü-spezifische Kernbereichsschutz im Verständnis des Zweiten Senats des BVerfG, in: HRRS 2013, S. 153 ff.

Roos, Jürgen/ Lenz, Thomas, Polizei- und Ordnungsbehördengesetz Rheinland-Pfalz, 4. Aufl. 2011 (zit.: Roos/ Lenz, POG).

Ruder, Karl-Heinz, Polizeirecht Baden-Württemberg, 8. Aufl. 2015 (zit: Ruder, Polizeirecht in Baden-Württemberg).

Rühle, Dietrich G., Polizei- und Ordnungsrecht für Rheinland-Pfalz, 5. Aufl. 2013 (zit.: Rühle, POG).

Rühle, Dietrich/ Suhr, Hans Jürgen, Polizei- und Ordnungsbehördengesetz Rheinland-Pfalz, Kommentar, 5. Aufl. 2012 (zit.: Rühle/ Suhr, POG)

Ruthig, Josef, Grundrechtlicher Kernbereich und Gefahrenabwehr: Verfahren, Rechtsschutz, Schadensersatz, in: Baumeister, Peter/ Roth, Wolfgang/ Ruthig, Josef (Hrsg.): Staat, Verwaltung und Rechtsschutz. Festschrift für Wolf-Rüdiger Schenke zum 70. Geburtstag, 2011, S. 499 ff. (zit.: Ruthig, Kernbereich).

Säcker, Franz Jürgen, TKG, Telekommunikationsgesetz, Kommentar, 3. Aufl. 2013 (zit.: Bearbeiter, in: Säcker, TKG).

Säcker, Hans Jürgen/ Rixecker, Roland (Hrsg.), Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 1, 7. Aufl. 2015 (zit.: Bearbeiter, in: MüKo BGB).

Sandkuhl, Heide u.a., Stellungnahme des Deutschen Anwaltvereins durch die Ausschüsse Gefahrenabwehrrecht zum Gesetzesentwurf der Landesregierung zur Änderung des Polizei- und Ordnungsbehördengesetzes Rheinland-Pfalz (LT-Drs. 15/4879), (zit.: Sandkuhl, Stellungnahme DAV), abrufbar unter: http://anwaltverein.de/downloads/stellungnahmen/SN-10/SN-69.pdf?PHPSESSID=6tf0j5f9oel5i8p70nn839cog1.

Schenke, Wolf-Rüdiger, Polizei- und Ordnungsrecht, 9. Aufl. 2016 (zit.: Schenke, POR).

Schenke, Wolf-Rüdiger, Verfassungsrechtliche Probleme polizeilichen Gewahrsams und polizeilicher Informationseingriffe, in: DVBl. 1996, S. 1393 ff.

Schenke, Wolf-Rüdiger/ Graulich, Kurt/ Ruthig, Josef, Sicherheitsrecht des Bundes, 2014 (zit.: Bearbeiter, in: Schenke/ Graulich/ Ruthig, Sicherheitsrecht des Bundes).

Schewe, Christoph S., Das Ende der präventiven Rasterfahndung zur Terrorismusbekämpfung?, in: NVwZ 2007, S. 174 ff.

Schmidbauer, Wilhelm/ Steiner, Udo (Hrsg.), Bayerisches Polizeiaufgabengesetz und Bayerisches Polizeiorganisationsgesetz, Kommentar, 4. Aufl. 2014 (zit.: Bearbeiter, in: Schmidbauer/ Steiner, BayPAG).

Schmidt-Keßeler, Nora, Verfassungswidrigkeit des § 160a Strafprozessordnung, in: DStR 2011, S. 1586 ff.

Schmidt-Räntsch, Jürgen, Deutsches Richtergesetz, Richterwahlgesetz, 6. Aufl. 2009 (zit.: Schmidt-Räntsch, DRiG).

Schneider, Franziska, Rechtliche Rahmenbedingungen für die Vornahme von Onlinedurchsuchungen. Onlinedurchsuchungen als Mittel zur Terrorismusbekämpfung in Deutschland und den USA, Dissertation, 2012 (zit.: Schneider, Onlinedurchsuchung).

Schneider, Hartmut, Zur Zulässigkeit strafprozessualer Begleitmaßnahmen im Zusammenhang mit dem Abhören des nicht öffentlich gesprochenen Wortes in Kraftfahrzeugen, in: NStZ 1999, S. 388 ff.

Schoch, Friedrich/ Schneider, Jens-Peter/ Bier, Wolfgang, Verwaltungsgerichtsordnung, Kommentar, Stand 30. Ergänzungslieferung 2016 (zit.: Bearbeiter, in: Schoch/ Schneider/ Bier, VwGO).

Schwabenbauer, Thomas, Kommunikationsschutz durch Art. 10 GG im digitalen Zeitalter, in: AöR 2012, S. 1 ff.

Seidl, Alexander/ Albrecht, Florian, Die polizeiliche Bestandsdatenauskunft in Hessen, in: VR 2014, S. 126 ff.

Shirvani, Foroud, Die Kontakt- und Begleitpersonen und die „Besonderen Mittel der Datenerhebung“ im Polizeirecht, in: VerwArch 2011, S. 86 ff.

Sieber, Ulrich, Stellungnahme zu dem Fragenkatalog des Bundesverfassungsgerichts in dem Verfahren 1 BvR 370/07 zum Thema der Onlinedurchsuchungen, Version 1.0 vom 9. Oktober 2007 (endg.) zur Anhörung in der mündlichen Verhandlung am 10. Oktober 2007. (zit.: Sieber, Stellungnahme).

Singelnstein, Tobias, Möglichkeiten und Grenzen neuerer strafprozessualer Ermittlungsmaßnahmen – Telekommunikation, Web 2.0, Datenbeschlagnahme, polizeiliche Datenverarbeitung & Co, in: NStZ 2012, S. 593 ff.

Skistims, Hendrik/ Roßnagel, Alexander, Rechtlicher Schutz vor Staatstrojanern? Verfassungsrechtliche Analyse einer Regierungs-Malware, in: ZD 2012, S. 3 ff.

Sodan, Helge/ Ziekow, Jan, Grundkurs Öffentliches Recht, 6. Aufl. 2014 (zit.: Sodan/ Ziekow, Grundkurs).

Sodan, Helge/ Ziekow, Jan, Verwaltungsgerichtsordnung, 3. Aufl. 2010 (zit.: Bearbeiter, in: Sodan/ Ziekow, VwGO).

Soiné, Michael, Eingriffe in informationstechnische Systeme nach dem Polizeirecht des Bundes und der Länder, in: NVwZ 2012, S. 1585 ff.

Späthe, Michael, Der Ausbau der informatorischen Polizeibefugnisse in Brandenburg, Dissertation, 2014 (zitiert: Späthe, Der Ausbau der informatorischen Polizeibefugnisse in Brandenburg).

Staats, Johann-Friedrich, Deutsches Richtergesetz, 2012 (zit.: Staats, DRiG).

Stadler, Thomas, Zulässigkeit der heimlichen Installation von Überwachungssoftware. Trennung von Onlinedurchsuchung und Quellen-Telekommunikationsüberwachung möglich?, in: MMR 2012, S. 18 ff.

Stephan, Ulrich/ Deger, Johannes, Polizeigesetz für Baden-Württemberg, Kommentar, 7. Aufl. 2014 (zit.: Stephan/ Deger, PolG BW).

Stern, Klaus/ Becker, Florian (Hrsg.), Grundrechte-Kommentar, 2. Aufl. 2016 (zit.: Bearbeiter, in: Stern/ Becker, GG).

Tetsch, Lambert Josef/ Baldaralli, Marcello (Hrsg.), Polizeigesetz des Landes Nordrhein-Westfalen, 2011 (zit.: Bearbeiter, in: Tetsch/ Baldaralli, PolG NRW).

Trurnit, Christoph, Polizeiliche Datenverarbeitung zur vorbeugenden Bekämpfung von Straftaten?, in: VBlBW 2011, S. 458 ff.

Vinken, Horst, Differenzierung zwischen RA und StB verfassungswidrig, in: DStR-KR 2012, S. 5 ff.

Volkmann, Uwe, Die Verabschiedung der Rasterfahndung als Mittel der vorbeugenden Verbrechensbekämpfung, in: JURA 2007, S. 132 ff.

Volkmann, Uwe, Das Aus der präventiven Rasterfahndung?!, in: JZ 2006, S. 918 ff.

Waechter, Kay, Bereitstellungspflicht für Fernmeldeanlagenbetreiber, in: VerwArch 1996, S. 68 ff.

Wiemers, Matthias, Anmerkung zu BVerfG, Urt. v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, in: NVwZ 2016, S. 839 ff.

Wildhagen, Lars, Persönlichkeitsschutz durch präventive Kontrolle. Richtervorbehalte und nichtrichterliche Kontrollorgane als Ausprägungen des Prinzips der Informationsoptimierung bei Grundrechtseingriffen, Dissertation, 2011 (zit.: Wildhagen, Persönlichkeitsschutz).

Wittmann, Antje, Gesetzgeber muss jetzt erst recht abwägen, in: AnwBl 2016, S. 497 ff.

Zabel, Benno, Terrorgefahr und Gesetzgebung. Zugleich eine kritische Auseinandersetzung mit der Neufassung des Bundeskriminalamtsgesetzes und deren Bedeutung für die straf- und polizeirechtliche Praxis, in: JR 2009, S. 453 ff.

Ziebarth, Wolfgang, Onlinedurchsuchung, Dissertation, 2013 (zit.: Ziebarth, Onlinedurchsuchung).

Ziekow, Jan/ Debus, Alfred G./ Piesker, Axel, Die Planung und Durchführung von Gesetzesevaluationen, 2013 (zit.: Ziekow/Debus/Piesker, Gesetzesevaluationen).

Anhang

I. Erhebungsbogen zu § 31 POG „Datenerhebung (durch den Einsatz technischer Mittel zur Überwachung und Aufzeichnung der Telekommunikation, Auskunft über Telekommunikation (ohne Quellen-TKÜ))“

1) *Bitte geben Sie hier die für die Durchführung der Maßnahme zuständige Polizeibehörde an!*

2) *Aus welchem Anlass wurden Daten durch den Einsatz technischer Mittel zur Überwachung und Aufzeichnung der Telekommunikation sowie durch Auskünfte über die Telekommunikation erhoben?*

☐ Abwehr einer gegenwärtigen Gefahr für Leib oder Leben einer Person

☐ bwehr einer gegenwärtigen Gefahr für Güter der Allgemeinheit (Bedrohung der Grundlagen oder des Bestands des Staates oder der Grundlagen der Existenz der Menschen)

Bitte beschreiben sie die zugrunde liegende Gefahrenlage mit einem Stichwort (z. B. „Entführung“)

3) *Welche Datenerhebungsmaßnahmen wurden **vor Anwendung** dieser Maßnahme ergriffen,*

   a) *zur Feststellung des Vorliegens einer gegenwärtigen Gefahr im Sinne von § 31 POG?*

   b) *als milderes Mittel zur Vermeidung von Maßnahmen nach § 31 POG?*

4) *Welche Vorkehrungen wurden getroffen, um den Schutz des Kernbereichs privater Lebensgestaltung sicherzustellen?*

Von der Datenerhebung betroffene Personen

5) Gegen wie viele Personen richtete sich die Maßnahme gemäß § 31 Abs. 1 POG nach dem Beschluss bzw. nach der Anordnung?

: nach § 4 verantwortliche Person(en)

: nach § 5 verantwortliche Person(en)

: in § 7 genannte(n) Person(en)

: Person(en), bei der/denen bestimmte Tatsachen die Annahme rechtfertigen, dass sie für die nach §§ 4 und 5 Verantwortlichen bestimmte oder herrührende Mitteilungen entgegennehmen oder weitergeben

6) Über wie viele Personen wurden im Zuge der Maßnahme gemäß § 31 Abs. 1 POG tatsächlich Daten erhoben?

(Personen gesamt)

davon Dritte:

7) Welche Daten wurden erhoben über

a) nach § 4 verantwortliche Person(en)?

☐ Telekommunikationsinhalte

☐ Verkehrsdaten

☐ keine Datenerhebung erfolgt

b) nach § 5 verantwortliche Person(en)?

☐ Telekommunikationsinhalte

☐ Verkehrsdaten

☐ keine Datenerhebung erfolgt

c) die in § 7 genannten Person(en)?

☐ Telekommunikationsinhalte

☐ Verkehrsdaten

☐ keine Datenerhebung erfolgt

d) über Personen, bei denen bestimmte Tatsachen die Annahme rechtfertigen, dass sie für die nach §§ 4 und 5 Verantwortlichen bestimmte oder herrührende Mitteilungen entgegennehmen oder weitergeben?

☐ Telekommunikationsinhalte

☐ Verkehrsdaten

☐ keine Datenerhebung erfolgt

e) über Dritte?

☐ Telekommunikationsinhalte

☐ Verkehrsdaten

☐ keine Datenerhebung erfolgt

8) Wurden auch Verkehrsdaten erhoben, die sich auf Zeiträume vor der Anordnung der Erhebungsmaßnahme erstrecken?

a) über nach § 4 verantwortliche Personen:

☐ ja

☐ nein

b) über nach § 5 verantwortliche Personen:

☐ ja

☐ nein

c) über die in § 7 genannten Personen:

☐ ja

☐ nein

d) über Personen, bei denen bestimmte Tatsachen die Annahme rechtfertigen, dass sie für die nach §§ 4 und 5 Verantwortlichen bestimmte oder herrührende Mitteilungen entgegennehmen oder weitergeben:

☐ ja

☐ nein

e) über Dritte?

☐ ja

☐ nein

Angaben zur angewendeten Maßnahme

9) Welchen Umfang hatte die Maßnahme? Bitte geben Sie die Art und Zahl der überwachten Anschlüsse an!

10) Wie viele Telekommunikationsverbindungen wurden während der Dauer der Maßnahme überwacht?

11) Gab es Probleme, z. B. technische Probleme, die den Erfolg der Maßnahme beeinträchtigt haben?

☐ ja

☐ nein

12) Falls ja, um was für Probleme hat es sich gehandelt?

☐ Gegenmaßnahmen des/der zu Überwachenden

☐ Technisches Equipment der Polizei nicht ausreichend

☐ Technisches Equipment allgemein (noch) nicht vorhanden

☐ Sonstiges:

13) Gab es Probleme im Zusammenhang mit der Ermöglichung der gewünschten Überwachung oder die Erteilung von Auskünften über Verkehrsdaten durch den/die Telekommunikationsdienstleister?

☐ Ja

☐ Nein

14) Falls ja, um was für Probleme hat es sich gehandelt?

Richterliche Entscheidung

15) Gab es Probleme bei der Einholung der richterlichen Entscheidung?

☐ Ja

☐ Nein

16) Falls ja, welche Probleme gab es?

17) Wie lang wurde die Maßnahme befristet?

18) Wurde die Maßnahme nach der ersten Befristung noch einmal verlängert?

☐ Ja

☐ Nein

19) Aus welchen Gründen wurde die Maßnahme verlängert?

20) Bis zu welcher Gesamtlänge wurde die Maßnahme bis zu ihrer Beendigung verlängert? (in Tagen)

21) Wie lang hat die Datenerhebung tatsächlich gedauert? (in Tagen)

22) Aus welchen Gründen wurde die Maßnahme beendet?

23) Wann wurde die Maßnahme abgeschlossen? Bitte hier das Datum angeben!

24) Wurde die Entscheidung von der Behördenleitung bzw. eines von ihr besonders beauftragten Beamten des höheren Dienstes wegen Gefahr im Verzug ohne vorherige Einholung einer richterlichen Entscheidung getroffen?

☐ Ja

☐ Nein **(→ weiter mit Frage 28)**

25) Falls ja, worauf wurde die Annahme einer Gefahr im Verzug gestützt?

26) In welchem zeitlichen Abstand zur Anordnung der Maßnahme durch die Behördenleitung etc. wurde die richterliche Entscheidung nachgeholt? (in Stunden)

27) Wurde die Anordnung durch die Behördenleitung vom OVG bestätigt?

☐ Ja

☐ Nein

Weiterverwendung der erhobenen Daten

28) Sind die Daten anschließend für andere Zwecke verwendet worden?

☐ Ja

☐ Nein **(→ weiter mit Frage 30)**

29) Falls ja, für welche Zwecke? (Mehrfachantworten möglich)

☐ Abwehr einer anderen dringenden Gefahr für die öffentliche Sicherheit

☐ Verfolgung einer besonders schweren Straftat,

<u>aus dem Strafgesetzbuch:</u>

☐ Straftaten des Friedensverrats, des Hochverrats und der Gefährdung des demokra tischen Rechtsstaates oder des Landesverrats und der Gefährdung der äußeren Sicherheit nach den §§ 80, 81, 82, nach den §§ 94, 95 Abs. 3 und § 96 Abs. 1, jeweils auch in Verbindung mit § 97 b, sowie nach den §§ 97 a, 98 Abs. 1 S. 2, § 99 Abs. 2 und den §§ 100, 100 a Abs. 4,

☐ Bildung krimineller Vereinigungen nach § 129 Abs. 1 in Verbindung mit Abs. 4 Halbsatz 2 und Bildung terroristischer Vereinigungen nach § 129 a Abs. 1, 2, 4, 5 S. 1 Alternative 1, jeweils auch in Verbindung mit § 129 b Abs. 1,

☐ Geldfälschung und Wertpapierfälschung in den Fällen der §§ 146, 151, jeweils auch in Verbindung mit § 152, gewerbs- oder bandenmäßige Fälschung von Zahlungskarten, Schecks und Wechseln nach § 152 a Abs. 3 und Fälschung von Zahlungskarten mit Garantiefunktion und Vordrucken für Euroschecks nach § 152 b Abs. 1 bis 4,

☐ Straftaten gegen die sexuelle Selbstbestimmung in den Fällen des § 176 a Abs. 2 Nr. 2 oder Abs. 3, § 177 Abs. 2 Nr. 2 oder § 179 Abs. 5 Nr. 2,

☐ Verbreitung, Erwerb und Besitz kinderpornografischer Schriften in den Fällen des § 184b Abs. 3,

☐ Mord und Totschlag nach §§ 211, 212,

☐ Straftaten gegen die persönliche Freiheit in den Fällen der §§ 234, 234 a Abs. 1, 2, §§ 239 a, 239 b und Menschenhandel zum Zweck der sexuellen Ausbeutung und zum Zweck der Ausbeutung der Arbeitskraft nach § 232 Abs. 3, 4 oder Abs. 5, § 233 Abs. 3, jeweils soweit es sich um Verbrechen handelt,

☐ Bandendiebstahl nach § 244 Abs. 1 Nr. 2 und schwerer Bandendiebstahl nach § 244,

☐ schwerer Raub nach § 250 Abs. 1 oder Abs. 2,

☐ räuberische Erpressung nach § 255 und besonders schwerer Fall einer Erpressung nach § 253 unter den in § 253 Abs. 4 S. 2 genannten Voraussetzungen,

☐ gewerbsmäßige Hehlerei, Bandenhehlerei und gewerbsmäßige Bandenhehlerei nach den §§ 260, 260 a,

☐ besonders schwerer Fall der Geldwäsche, Verschleierung unrechtmäßig erlangter Vermögenswerte nach § 261 unter den in § 261 Abs. 4 S. 2 genannten Voraussetzungen,

☐ besonders schwerer Fall der Bestechlichkeit und Bestechung nach § 335 Abs. 1 unter den in § 335 Abs. 2 Nr. 1 bis 3 genannten Voraussetzungen,

aus dem Asylverfahrensgesetz:

☐ Verleitung zur missbräuchlichen Asylantragstellung nach § 84 Abs. 3,

☐ gewerbs- und bandenmäßige Verleitung zur missbräuchlichen Asylantragstellung nach § 84 a Abs. 1,

aus dem Aufenthaltsgesetz:

☐ Einschleusen von Ausländern nach § 96 Abs. 2,

☐ gewerbs- und bandenmäßiges Einschleusen nach § 97,

aus dem Betäubungsmittelgesetz:

☐ besonders schwerer Fall einer Straftat nach § 29 Abs. 1 S. 1 Nr. 1, 5, 6, 10, 11 oder 13 in Verbindung mit § 29 Abs. 3 S. 2 Nr. 1,

☐ eine Straftat nach §§ 29 a, 30 Abs. 1 Nr. 1, 2, 4, § 30 a,

aus dem Gesetz über die Kontrolle von Kriegswaffen:

☐ eine Straftat nach § 19 Abs. 2 oder § 20 Abs. 1, jeweils auch in Verbindung mit § 21,

☐ besonders schwerer Fall einer Straftat nach § 22 a Abs. 1 in Verbindung mit Abs. 2,

aus dem Völkerstrafgesetzbuch:

☐ Völkermord nach § 6,

☐ Verbrechen gegen die Menschlichkeit nach § 7,

☐ Kriegsverbrechen nach den §§ 8 bis 12,

aus dem Waffengesetz:

☐ besonders schwerer Fall einer Straftat nach § 51 Abs. 1 in Verbindung mit Abs. 2,

☐ besonders schwerer Fall einer Straftat nach § 52 Abs. 1 Nr. 1 in Verbindung mit Abs. 5.

Erfolg der Maßnahme

30) Konnte die Maßnahme zur Erhärtung eines Gefahren- bzw. Straftatenverdachtes beitragen?

☐ Ja

☐ Nein

31) Konnten durch die Maßnahme Hinweise auf weitere dringende Gefahren bzw. besonders schwere Straftaten gewonnen werden?

☐ Ja

☐ Nein

32) Konnte die Maßnahme zur Verhinderung einer Gefahr/Straftat beitragen?

☐ Ja

☐ Nein

☐ Nicht eindeutig feststellbar

33) Konnte die Maßnahme zur Aufklärung einer Straftat beitragen?

☐ Ja

☐ Nein

☐ Verfahren läuft noch

34) Wie bewerten sie in diesem konkreten Fall den Nutzen der erhobenen Daten?

- ☐ Sehr hoch
- ☐ Hoch
- ☐ Teil/teils
- ☐ Gering
- ☐ Sehr gering

35) Wurden parallel zur hier genannten Maßnahme weitere Datenerhebungsmaßnahmen durchgeführt?

- ☐ Ja
- ☐ Nein (→ weiter mit Frage 37)

36) Falls ja, welche?

37) Wie ist der Stand des Verfahrens?

- ☐ Das Verfahren ist eingestellt worden.
- ☐ Das Verfahren ist an die Staatsanwaltschaft abgegeben worden und wird dort weiter geführt.
- ☐ Das Verfahren ist an die Staatsanwaltschaft abgegeben worden und ist dann ohne Verurteilung eingestellt worden.
- ☐ Das Verfahren ist an die Staatsanwaltschaft abgegeben worden und mit einer Verurteilung abgeschlossen worden.
- ☐ Der Vorgang ist erledigt.

Unterrichtung der betroffenen Personen

38) Sind die Personen, gegen die sich die Maßnahme gerichtet hat, nach Abschluss der Maßnahme unterrichtet worden?

- ☐ Ja
- ☐ Nein (→ weiter mit Frage 40)

39) Falls ja, wie lange hat es gedauert, bis die Personen, gegen die sich die Maßnahme gerichtet hat, unterrichtet wurden?

(Zeitraum zwischen Abschluss der Maßnahme und Unterrichtung in Tagen)

40) Falls nein, aus welchen Gründen sind diese Personen nicht unterrichtet worden?

- ☐ Gefahr für Leib, Leben oder Freiheit einer Person
- ☐ Gefahr für besondere Vermögenswerte
- ☐ Gefahr für den Zweck der Maßnahme
- ☐ Anschluss eines strafrechtlichen Ermittlungsverfahrens gegen den Betroffenen an den die Maßnahme auslösenden Sachverhalt
- ☐ Notwendigkeit der Erhebung weiterer Daten über die betroffene Person, um diese zu identifizieren (ohne dass dies im Interesse der betroffenen Person geboten erscheint)
- ☐ Keine Erstellung von Aufzeichnungen mit personenbezogenen Daten
- ☐ Unverzügliche Vernichtung der personenbezogenen Daten nach Beendigung der Maßnahme
- ☐ Sonstiges:

41) Wie häufig bedurfte die Zurückstellung der Unterrichtung einer richterlichen Zustimmung?

(Mal)

42) Sind die sonstigen betroffenen Personen, über die Daten erhoben wurden, nach Abschluss der Maßnahme unterrichtet worden?

- ☐ Ja
- ☐ Nein
- ☐ Es sind keine Daten über sonstige betroffene Personen erhoben worden.

43) Falls ja, wie lange hat es gedauert, bis diese sonstigen betroffenen Personen unterrichtet wurden?

(Zeitraum zwischen Abschluss der Maßnahme und Unterrichtung in Tagen)

*44) Falls nein, aus welchen Gründen sind diese sonstigen betroffenen Personen **nicht** unterrichtet worden?*

- ☐ Gefahr für Leib, Leben oder Freiheit einer Person
- ☐ Gefahr für besondere Vermögenswerte
- ☐ Gefahr für den Zweck der Maßnahme
- ☐ Anschluss eines strafrechtlichen Ermittlungsverfahrens gegen den Betroffenen an den die Maßnahme auslösenden Sachverhalt
- ☐ Notwendigkeit der Erhebung weiterer Daten über die betroffene Person, um diese zu identifizieren (ohne dass dies im Interesse der betroffenen Person geboten erscheint)
- ☐ Keine Erstellung von Aufzeichnungen mit personenbezogenen Daten

☐ Unverzügliche Vernichtung der personenbezogenen Daten nach Beendigung der Maßnahme

☐ Sonstiges:

45) *Falls Sie inhaltliche Anmerkungen oder Kommentare zu diesem Fall haben, können Sie hierfür das Freitextfeld nutzen!*

II. Erhebungsbogen zu § 31b POG „Auskunft über Nutzungsdaten“

1) Bitte geben Sie hier die für die Durchführung der Maßnahme zuständige Polizeibehörde an!

2) Aus welchem Anlass haben Sie Auskunft über Nutzungsdaten (§ 15 Abs.1 des Telemediengesetzes) verlangt?

☐ Abwehr einer Gefahr für Leib oder Leben einer Person

☐ Abwehr einer Gefahr für Güter der Allgemeinheit (Bedrohung der Grundlagen oder des Bestands des Staates oder der Grundlagen der Existenz der Menschen)

Bitte beschreiben sie die zugrunde liegende Gefahrenlage mit einem Stichwort (z. B. „Entführung“)

*3) Welche Datenerhebungsmaßnahmen wurden **vor Anwendung** dieser Maßnahme ergriffen,*

a) zur Feststellung des Vorliegens einer Gefahr im Sinne von § 31b POG?

b) als milderes Mittel zur Vermeidung von Maßnahmen nach § 31b POG?

4) Welche Vorkehrungen wurden getroffen, um den Schutz des Kernbereichs privater Lebensgestaltung sicherzustellen?

Von der Datenerhebung betroffene Personen

5) Gegen wie viele Personen richtete sich die Maßnahme gemäß § 31b POG nach dem Beschluss bzw. nach der Anordnung?

: nach § 4 verantwortliche Person(en)

: nach § 5 verantwortliche Person(en)

: in § 7 genannte(n) Person(en)

: Person(en), bei der/denen bestimmte Tatsachen die Annahme rechtfertigen, dass sie für die nach §§ 4 und 5 Verantwortlichen bestimmte oder herrührende Mitteilungen entgegennehmen oder weitergeben

6) Über wie viele Personen wurden im Zuge der Maßnahme gemäß § 31b POG tatsächlich Daten erhoben?

(Personen gesamt)

davon Dritte:

7) Welche Daten wurden erhoben über

a) nach § 4 verantwortliche Person(en)?

- ☐ Merkmale zur Identifikation des Nutzers,
- ☐ Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und
- ☐ Angaben über die vom Nutzer in Anspruch genommenen Telemedien
- ☐ Sonstige:
- ☐ keine Datenerhebung erfolgt

b) nach § 5 verantwortliche Person(en)?

- ☐ Merkmale zur Identifikation des Nutzers,
- ☐ Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und
- ☐ Angaben über die vom Nutzer in Anspruch genommenen Telemedien
- ☐ Sonstige:
- ☐ keine Datenerhebung erfolgt

c) die in § 7 genannte(n) Person(en)?

- ☐ Merkmale zur Identifikation des Nutzers,
- ☐ Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und
- ☐ Angaben über die vom Nutzer in Anspruch genommenen Telemedien
- ☐ Sonstige:
- ☐ keine Datenerhebung erfolgt

d) über Personen, bei denen bestimmte Tatsachen die Annahme rechtfertigen, dass sie für die nach §§ 4 und 5 Verantwortlichen bestimmte oder herrührende Mitteilungen entgegennehmen oder weitergeben?

- ☐ Merkmale zur Identifikation des Nutzers,
- ☐ Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und
- ☐ Angaben über die vom Nutzer in Anspruch genommenen Telemedien
- ☐ Sonstige:
- ☐ keine Datenerhebung erfolgt

e) Über Dritte?

- ☐ Merkmale zur Identifikation des Nutzers,
- ☐ Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und
- ☐ Angaben über die vom Nutzer in Anspruch genommenen Telemedien
- ☐ Sonstige:
- ☐ keine Datenerhebung erfolgt

8) Wurde die Auskunft auch über zukünftige Nutzungsdaten angeordnet?

a) Über nach § 4 verantwortliche Personen:

- ☐ Ja
- ☐ Nein

b) Über nach § 5 verantwortliche Personen:

- ☐ Ja
- ☐ Nein

c) Über die in § 7 genannte(n) Personen:

- ☐ Ja
- ☐ Nein

d) über Personen, bei denen bestimmte Tatsachen die Annahme rechtfertigen, dass sie für die nach §§ 4 und 5 Verantwortlichen bestimmte oder herrührende Mitteilungen entgegennehmen oder weitergeben:

- ☐ Ja
- ☐ Nein

e) Über Dritte?

- ☐ Ja
- ☐ Nein

Angaben zur angewendeten Maßnahme

9) Welchen Umfang hatte die Maßnahme? Bitte geben Sie an, über wie viele und welche elektronischen Informations- und Kommunikationsdienste Nutzungsdaten erhoben wurden!

10) *Gab es Probleme, z. B. technische Probleme, die den Erfolg der Maßnahme beeinträchtigt haben?*

- ☐ Ja
- ☐ Nein

11) *Falls ja, um was für Probleme hat es sich gehandelt?*

- ☐ Gegenmaßnahmen des/der zu Überwachenden
- ☐ Technisches Equipment der Polizei nicht ausreichend
- ☐ Technisches Equipment allgemein (noch) nicht vorhanden
- ☐ Sonstiges:

12) *Gab es Probleme im Zusammenhang mit der Bereitstellung der gewünschten Daten durch den/die Telemediendienstleister?*

- ☐ Ja
- ☐ Nein

13) *Falls ja, um was für Probleme hat es sich gehandelt?*

Richterliche Entscheidung

14) *Gab es Probleme bei der Einholung der richterlichen Entscheidung?*

- ☐ Ja
- ☐ Nein

15) *Falls ja, welche Probleme gab es?*

16) *Wie lang wurde die Maßnahme befristet?*

17) *Wurde die Maßnahme nach der ersten Befristung noch einmal verlängert?*

- ☐ Ja
- ☐ Nein

18) Aus welchen Gründen wurde die Maßnahme verlängert?

19) Bis zu welcher Gesamtlänge wurde die Maßnahme bis zu ihrer Beendigung verlängert? (in Tagen)

20) Wie lang hat die Datenerhebung tatsächlich gedauert? (in Tagen)

21) Aus welchen Gründen wurde die Maßnahme beendet?

22) Wann wurde die Maßnahme abgeschlossen? Bitte hier das Datum angeben!

23) Wurde die Entscheidung von der Behördenleitung bzw. eines von ihr besonders beauftragten Beamten des höheren Dienstes wegen Gefahr im Verzug ohne vorherige Einholung einer richterlichen Entscheidung getroffen?

☐ Ja

☐ Nein (→ weiter mit Frage 27)

24) Falls ja, worauf wurde die Annahme einer Gefahr im Verzug gestützt?

25) In welchem zeitlichen Abstand zur Anordnung der Maßnahme durch die Behördenleitung etc. wurde die richterliche Entscheidung nachgeholt?(in Stunden)

26) Wurde die Anordnung durch die Behördenleitung vom OVG bestätigt?

☐ Ja

☐ Nein

Weiterverwendung der erhobenen Daten

27) Sind die Daten anschließend für andere Zwecke verwendet worden?

☐ Ja

☐ Nein (→ weiter mit Frage 29)

28) Falls ja, für welche Zwecke? (Mehrfachantworten möglich)

☐ Abwehr einer anderen dringenden Gefahr für die öffentliche Sicherheit

☐ Verfolgung einer besonders schweren Straftat und zwar:

aus dem Strafgesetzbuch:

☐ Straftaten des Friedensverrats, des Hochverrats und der Gefährdung des demokratischen Rechtsstaates oder des Landesverrats und der Gefährdung der äußeren Sicherheit nach den §§ 80, 81, 82, nach den §§ 94, 95 Abs. 3 und § 96 Abs. 1, jeweils auch in Verbindung mit § 97 b, sowie nach den §§ 97 a, 98 Abs. 1 S. 2, § 99 Abs. 2 und den §§ 100, 100 a Abs. 4,

☐ Bildung krimineller Vereinigungen nach § 129 Abs. 1 in Verbindung mit Abs. 4 Halbsatz 2 und Bildung terroristischer Vereinigungen nach § 129 a Abs. 1, 2, 4, 5 S. 1 Alternative 1, jeweils auch in Verbindung mit § 129 b Abs. 1,

☐ Geldfälschung und Wertpapierfälschung in den Fällen der §§ 146, 151, jeweils auch in Verbindung mit § 152, gewerbs- oder bandenmäßige Fälschung von Zahlungskarten, Schecks und Wechseln nach § 152 a Abs. 3 und Fälschung von Zahlungskarten mit Garantiefunktion und Vordrucken für Euroschecks nach § 152 b Abs. 1 bis 4,

☐ Straftaten gegen die sexuelle Selbstbestimmung in den Fällen des § 176 a Abs. 2 Nr. 2 oder Abs. 3, § 177 Abs. 2 Nr. 2 oder § 179 Abs. 5 Nr. 2,

☐ Verbreitung, Erwerb und Besitz kinderpornografischer Schriften in den Fällen des § 184b Abs. 3,

☐ Mord und Totschlag nach §§ 211, 212,

☐ Straftaten gegen die persönliche Freiheit in den Fällen der §§ 234, 234 a Abs. 1, 2, §§ 239 a, 239 b und Menschenhandel zum Zweck der sexuellen Ausbeutung und zum Zweck der Ausbeutung der Arbeitskraft nach § 232 Abs. 3, 4 oder Abs. 5, § 233 Abs. 3, jeweils soweit es sich um Verbrechen handelt,

☐ Bandendiebstahl nach § 244 Abs. 1 Nr. 2 und schwerer Bandendiebstahl nach § 244,

☐ schwerer Raub nach § 250 Abs. 1 oder Abs. 2,

☐ räuberische Erpressung nach § 255 und besonders schwerer Fall einer Erpressung nach § 253 unter den in § 253 Abs. 4 S. 2 genannten Voraussetzungen,

☐ gewerbsmäßige Hehlerei, Bandenhehlerei und gewerbsmäßige Bandenhehlerei nach den §§ 260, 260 a,

☐ besonders schwerer Fall der Geldwäsche, Verschleierung unrechtmäßig erlangter Vermögenswerte nach § 261 unter den in § 261 Abs. 4 S. 2 genannten Voraussetzungen,

☐ besonders schwerer Fall der Bestechlichkeit und Bestechung nach § 335 Abs. 1 unter den in § 335 Abs. 2 Nr. 1 bis 3 genannten Voraussetzungen,

aus dem Asylverfahrensgesetz:

☐ Verleitung zur missbräuchlichen Asylantragstellung nach § 84 Abs. 3,

☐ gewerbs- und bandenmäßige Verleitung zur missbräuchlichen Asylantragstellung nach § 84 a Abs. 1,

aus dem Aufenthaltsgesetz:

☐ Einschleusen von Ausländern nach § 96 Abs. 2,

☐ gewerbs- und bandenmäßiges Einschleusen nach § 97,

aus dem Betäubungsmittelgesetz:

☐ besonders schwerer Fall einer Straftat nach § 29 Abs. 1 S. 1 Nr. 1, 5, 6, 10, 11 oder 13 in Verbindung mit § 29 Abs. 3 S. 2 Nr. 1,

☐ eine Straftat nach §§ 29 a, 30 Abs. 1 Nr. 1, 2, 4, § 30 a,

aus dem Gesetz über die Kontrolle von Kriegswaffen:

☐ eine Straftat nach § 19 Abs. 2 oder § 20 Abs. 1, jeweils auch in Verbindung mit § 21,

☐ besonders schwerer Fall einer Straftat nach § 22 a Abs. 1 in Verbindung mit Abs. 2,

aus dem Völkerstrafgesetzbuch:

☐ Völkermord nach § 6,

☐ Verbrechen gegen die Menschlichkeit nach § 7,

☐ Kriegsverbrechen nach den §§ 8 bis 12,#

aus dem Waffengesetz:

☐ besonders schwerer Fall einer Straftat nach § 51 Abs. 1 in Verbindung mit Abs. 2,

☐ besonders schwerer Fall einer Straftat nach § 52 Abs. 1 Nr. 1 in Verbindung mit Abs. 5.

Erfolg der Maßnahme

29) *Konnte die Maßnahme zur Erhärtung eines Gefahren- bzw. Straftatenverdachtes beitragen?*

- ☐ Ja
- ☐ Nein

30) *Konnten durch die Maßnahme Hinweise auf weitere dringende Gefahren bzw. besonders schwere Straftaten gewonnen werden?*

- ☐ Ja
- ☐ Nein

31) *Konnte die Maßnahme zur Verhinderung einer Gefahr/Straftat beitragen?*

- ☐ Ja
- ☐ Nein
- ☐ Nicht eindeutig feststellbar

32) *Konnte die Maßnahme zur Aufklärung einer Straftat beitragen?*

- ☐ Ja
- ☐ Nein
- ☐ Verfahren läuft noch

33) *Wie bewerten sie in diesem konkreten Fall den Nutzen der erhobenen Daten?*

- ☐ Sehr hoch
- ☐ Hoch
- ☐ Teil/teils
- ☐ Gering
- ☐ Sehr gering

34) *Bitte erläutern Sie Ihre Bewertung kurz, soweit dies datenschutzrechtlich und ermittlungstaktisch möglich ist!*

35) Wurden parallel zur hier genannten Maßnahme weitere Datenerhebungsmaßnahmen durchgeführt?

☐ *Ja*

☐ *Nein (→ weiter mit Frage 37)*

36) Falls ja, welche?

37) Wie ist der Stand des Verfahrens?

☐ Das Verfahren ist eingestellt worden.

☐ Das Verfahren ist an die Staatsanwaltschaft abgegeben worden und wird dort weitergeführt.

☐ Das Verfahren ist an die Staatsanwaltschaft abgegeben worden und ist dann ohne Verurteilung eingestellt worden.

☐ Das Verfahren ist an die Staatsanwaltschaft abgegeben worden und mit einer Verurteilung abgeschlossen worden.

☐ Der Vorgang ist erledigt.

Unterrichtung der betroffenen Personen

38) Sind die Personen, gegen die sich die Maßnahme gerichtet hat, nach Abschluss der Maßnahme unterrichtet worden?

☐ Ja

☐ Nein (→ weiter mit Frage 40)

39) Falls ja, wie lange hat es gedauert, bis die Personen, gegen die sich die Maßnahme gerichtet hat, unterrichtet wurden?

(Zeitraum zwischen Abschluss der Maßnahme und Unterrichtung in Tagen)

40) Falls nein, aus welchen Gründen sind diese Personen nicht unterrichtet worden?

☐ Gefahr für Leib, Leben oder Freiheit einer Person

☐ Gefahr für besondere Vermögenswerte

☐ Gefahr für den Zweck der Maßnahme

☐ Anschluss eines strafrechtlichen Ermittlungsverfahrens gegen den Betroffenen an den die Maßnahme auslösenden Sachverhalt

- ☐ Notwendigkeit der Erhebung weiterer Daten über die betroffene Person, um diese zu identifizieren (ohne dass dies im Interesse der betroffenen Person geboten erscheint)
- ☐ Keine Erstellung von Aufzeichnungen mit personenbezogenen Daten
- ☐ Unverzügliche Vernichtung der personenbezogenen Daten nach Beendigung der Maßnahme
- ☐ Sonstiges:

41) Wie häufig bedurfte die Zurückstellung der Unterrichtung einer richterlichen Zustimmung?

(Mal)

42) Sind die sonstigen betroffenen Personen, über die Daten erhoben wurden, nach Abschluss der Maßnahme unterrichtet worden?

- ☐ Ja
- ☐ Nein (→ weiter mit Frage 44)
- ☐ Es sind keine Daten über sonstige betroffene Personen erhoben worden.

43) Falls ja, wie lange hat es gedauert, bis diese sonstigen betroffenen Personen unterrichtet wurden?

(Zeitraum zwischen Abschluss der Maßnahme und Unterrichtung in Tagen)

44) Falls nein, aus welchen Gründen sind diese sonstigen betroffenen Personen nicht unterrichtet worden?

- ☐ Gefahr für Leib, Leben oder Freiheit einer Person
- ☐ Gefahr für besondere Vermögenswerte
- ☐ Gefahr für den Zweck der Maßnahme
- ☐ Anschluss eines strafrechtlichen Ermittlungsverfahrens gegen den Betroffenen an den die Maßnahme auslösenden Sachverhalt
- ☐ Notwendigkeit der Erhebung weiterer Daten über die betroffene Person, um diese zu identifizieren (ohne dass dies im Interesse der betroffenen Person geboten erscheint)
- ☐ Keine Erstellung von Aufzeichnungen mit personenbezogenen Daten
- ☐ Unverzügliche Vernichtung der personenbezogenen Daten nach Beendigung der Maßnahme
- ☐ Sonstiges:

45) Falls Sie inhaltliche Anmerkungen oder Kommentare zu diesem Fall haben, können Sie hierfür das Freitextfeld nutzen!

III. Interviewleitfaden für die Polizeibehörden

A. Datenerhebungsmaßnahmen

1) **§ 29 POG** „Datenerhebung durch den verdeckten Einsatz technischer Mittel in oder aus Wohnungen
2) **§ 31 POG** „Datenerhebung durch den Einsatz technischer Mittel zur Überwachung und Aufzeichnung der Telekommunikation, Auskunft über Telekommunikation (ohne Quellen-TKÜ)
3) **§ 31 Abs. 3 POG** „Datenerhebung durch den Einsatz technischer Mittel zur Überwachung und Aufzeichnung der Telekommunikation (Quellen-TKÜ)
4) **§ 31 b POG** „Auskunft über Nutzungsdaten“
5) **§ 31 c POG** „Datenerhebung durch den Einsatz technischer Mittel in informationstechnischen Systemen“
6) **§ 31 e POG** „Funkzellenabfrage“
7) **§ 38 POG** „Besondere Formen des Datenabgleichs“

B. Nutzen der Datenerhebungsmaßnahmen

1) Wie bewerten Sie insgesamt den Nutzen der gesetzlichen Zurverfügungstellung der o.g. Maßnahmen für Ihre Arbeit (auch wenn die Maßnahme nicht zum Einsatz kam)? Bitte begründen Sie Ihre Einschätzung kurz!
2) Welche Vorteile haben die hier betrachteten Datenerhebungsmaßnahmen gegenüber anderen Maßnahmen?
3) Welche Nachteile sehen Sie bei diesen Datenerhebungsmaßnahmen?

C. Anwendungserfahrungen und Optimierungsmöglichkeiten

1) Wie beurteilen Sie insgesamt die Anwendbarkeit der Regelungen in der polizeilichen Praxis? Bitte begründen Sie Ihre Einschätzung kurz!
   - Gibt es aus Ihrer Sicht Probleme (z.B. technischer oder rechtlicher Art oder hinsichtlich des Vorliegens der Tatbestandsvoraussetzungen) bei der Durchführung dieser Maßnahme? Falls ja, welche?
   - Wie unterscheiden Sie bei der Datenerhebung zwischen Nichtstörern und Dritten?
2) Welche Gründe gibt es Ihrer Meinung nach dafür, dass die Datenerhebungsmaßnahmen bislang nur selten bzw. überhaupt nicht zur Anwendung gekommen sind?
3) Welche Überlegungen haben in den Fällen, in denen Datenerhebungsmaßnahmen gemäß § 31 POG zum Einsatz kamen, zur Ausübung des Ermessens zugunsten der Beantragung der Maßnahme geführt? (nur bei PP Koblenz, Mainz und Rheinpfalz)
4) Wie bewerten Sie die Aussagekraft der gemäß § 31 POG erhobenen Daten im Allgemeinen? Bitte begründen Sie Ihre Einschätzung kurz! (nur bei PP Koblenz, Mainz und Rheinpfalz)

5) Sind Ihnen Fälle in Ihrem Zuständigkeitsbereich bekannt, in denen die Durchführung der o.g. Datenerhebungsmaßnahmen erwogen wurde, ohne dass die Maßnahme tatsächlich zum Einsatz gekommen ist?

   - Falls ja, aus welchen Gründen ist von der Durchführung der Datenerhebungsmaßnahme Abstand genommen worden?
   - Wurden stattdessen andere Maßnahmen ergriffen? Falls ja, welche?

6) Sind Ihnen Fälle in Ihrem Zuständigkeitsbereich bekannt, in denen die o.g. Datenerhebungsmaßnahmen beantragt wurden, das OVG jedoch seine Zustimmung hierzu verweigerte?

   - Falls ja, wie oft ist dies seit Inkrafttreten der Neuregelungen im Jahr 2011 vorgekommen?
   - Aus welchen Gründen ist die richterliche Zustimmung verweigert worden?
   - Wie oft ist dies vor Inkrafttreten der Neureglungen im Jahr 2011 vorgekommen?
   - Aus welchen Gründen ist die richterliche Zustimmung verweigert worden?

7) Wie bewerten Sie die Neuregelung von 2011 im Vergleich zur vorherigen Regelung? Bitte begründen Sie ihre Einschätzung kurz!

8) Welche konkreten Optimierungsmöglichkeiten sehen Sie bei den o.g. Datenerhebungsmaßnahmen, die Ihre Arbeit erleichtern könnten?

D. Abschließende Fragen

1) Welche Dienstvorschriften existieren zur Anwendung der Datenerhebungsmaßnahmen?

2) Wie stellen Sie bei den o.g. Maßnahmen sicher, dass die Zahl der nichtbetroffenen Dritten, von denen Daten erhoben werden, möglichst klein gehalten wird? Durch welche zusätzlichen Maßnahmen (z.B. frühzeitige Löschung, besondere Datensicherung u.ä.) versuchen Sie, nach Möglichkeit eine Verringerung der Belastung der Betroffenen zu erreichen?

3) Beispielsweise wegen des Vorliegens der Ausnahmen gemäß § 40 Abs. 5 und 6 POG unterbleibt ggf. eine Unterrichtung der von Datenerhebungsmaßnahmen Betroffenen selbst dann, wenn zahlreiche personenbeziehbare Daten erhoben worden sind. Hierzu wird aus Sicht des Datenschutzes vorgeschlagen, dass in diesen Fällen - nach Abschluss der Maßnahme, wenn ein Ermittlungserfolg nicht mehr gefährdet werden würde - zur Kompensation der unterbliebenen Unterrichtungen darüber öffentlich zu informieren ist bzw. dass dann zumindest der Landesdatenschutzbeauftragte oder das Parlament zu unterrichten sind. Wie beurteilen Sie diesen Vorschlag?

4) Die Datenerhebungsmaßnahmen nach POG existieren auch in der StPO. Nach welchen Gesichtspunkten entscheiden Sie in der Praxis, bis zu welchem Zeitpunkt Sie präventiv auf der Grundlage des POG und ab wann Sie im Rahmen der Strafverfolgung nach der StPO tätig werden? Wie häufig kommen die entsprechenden Datenerhebungsmaßnahmen nach StPO im Vergleich zu denen nach POG zur Anwendung?

5) Halten Sie es für sinnvoll, eine einheitliche Gerichtszuständigkeit für die o.g. Maßnahmen zu schaffen? Falls ja, welches Gericht/welche Gerichte sollte(n) zuständig sein? Wie kommen Sie zu dieser Einschätzung?

6) Gibt es aus Ihrer Sicht andere Datenerhebungsmaßnahmen, die gesetzlich geregelt werden sollten? Falls ja, welche und warum?

IV. Synopse der Polizeigesetze der Länder sowie des BKAG und der StPO

Ebene	Polizeige-setze	§ 29 POG	§ 31 I, II POG	§ 31 III POG	§ 31 VI POG	§ 31b POG	§ 31c POG	§ 31e POG	§ 38 POG	§ 39a POG	§ 39b POG	§ 40 V, VI POG
Baden-Württemberg	PolG	§ 23	§ 23a	-	§ 23a V	§ 23a I	-	§ 23a II 6	§ 40	§ 23 II, V	§ 9a	§§ 23 VI, 40 V
Bayern	BayPAG	Art. 34	Art. 34a-c	-	Art. 34b	-	Art. 34d	Art. 34c III 2	Art. 44	Art. 34 II, V, VII, 34a I, 34c IV, VI, 34d I, IV, V, VI	Art. 34 I, III, V, VIII, Art. 34a I, 34c IV, 34d I, IV, V	Art. 34 VI, Art. 34c V, Art. 34d VII, 44 V
Berlin	ASOG Bln	§ 25 IVa-X	-	-	-	-	-	-	§ 47	§ 25 IVa	§ 25 IVa	§ 25 VII, VIIa
Brandenburg	BbgPolG	§ 33a	§ 33b	-	§ 33b VI, VII	33b VI, VII	-	-	§ 46	§§ 29 VI, 33a III, V, 33b II	§§ 33a II, 33b II	§§ 29 VII, VIII, 46 V
Bremen	BremPolG	§ 33 II-IX	-	-	-	-	-	-	§ 36i	§ 33 IV	§ 33 IX	§ 33 V
Hamburg	PolDVG HA	§ 10a	§§ 10b, e	§§ 10c, e	§§ 10b III, 10d IV	-	-	§ 10e II 2	§ 23	§§ 10 III, 10a V, VII, 10e III, V	§ 10 III	§§ 10a VI, 23 V
Hessen	HSOG	§ 15 IV-IX	§ 15a	§ 15b	§ 15a I, II, VI	-	-	-	§ 26	§§ 15 IV, V, 27 II, III	§ 21 II	§ 29 VI, VII
Mecklenburg-Vor-pommern	SOG M-V	§§ 34, 34b	§ 34a	-	§ 34a VI-IX	-	-	-	§ 44	§§ 34a VIII, 34b II, III, VI	§ 33 VI	§§ 34a VII, § 34b VIII
Niedersachsen	Nds. SOG	§ 35a	§ 33a	-	§ 33a II, VII	-	-	-	§ 45a	§§ 33a III, 35a II, III	§ 30 VII	§ 30 IV-VI
NRW	PolG NRW	§ 18	-	-	§ 20a	§ 20a	-	-	§ 31	§§ 16, 18 III, IV	§§ 16 V, 18 III	§§ 17 V, VI, § 31 V
Saarland	SPolG	§ 28a	§ 28b	-	§ 28c	-	-	-	§ 37	§ 28d	§ 28d I	§ 28 V
Sachsen	SächsPolG	§ 41	-	-	-	-	-	-	§ 47	§ 41 VI, VII	§ 41 VI	§§ 41 VIII, 47 V
Sachsen-Anhalt	SOG LSA	§ 17 IV-VI	§§ 17a, b		§§ 17a III, §17b VI	-	-	-	§ 31	§ 17 IVa-c	§ 17 IVd	§§ 17 VII, § 31 V
Schleswig-Holstein	LVwG	§§ 185, 186-186b	§§ 185a, 186	-	§§ 185a IV, 186a VII	§ 180a IV	-	§ 185a II, III	§ 195a	§ 186a I-III	§ 186a IV	§§ 186 IV, V, 195 V
Thüringen	ThürPAG	§ 35	§§ 34a, b	§ 34a II	§ 34a VII	§ 34b II	-	-	§ 44	§§ 34a I, IV, 35 II, VI, 36 II	§§ 34a I, IV, 34b I, 35 II, IV, 36 II	§§ 36 III, 44 V
Bund	BKAG	§ 20h	§ 20l	§ 20l II	§ 20l III, V, VI	§ 20m II	§ 20k	§ 20m III 2	§ 20j	§§ 16 Ia, 20h V	§ 20u	§ 20w
Bund	StPO	§§ 100c-e	§§ 100a, b	-	§§ 100b III, 100j	-	-	§ 100g III	§§ 98a-c	§§ 100a IV, 100c IV, V, VII	§§ 100c VI, 160a	-

I. SPEYERER FORSCHUNGSBERICHTE

(institutseigene Reihe, über das Institut zu beziehen)

Nr. 269 *Gisela Färber* (Hrsg.), Governing from the Center: The Influence of the Federal/Central Government on Subnational Governments. Papers Presented at the Conference of the IACFS September 29 – October 1, 2011 in Speyer, September 2012.

Nr. 270 *Sabine Kuhlmann/Philipp Richter/Christian Schwab/Dirk Zeitz*: Kommunal- und Verwaltungsreform: Optionen zur Neugestaltung der Gemeindeebene in Brandenburg, September 2012.

Nr. 271 *Gisela Färber/Joachim Wieland/Marco Salm/Johanna Wolff/Dirk Zeitz*, Reform des kommunalen Finanzausgleichs in Thüringen. Gutachten im Auftrag des Finanzministeriums des Freistaats Thüringen, November 2012.

Nr. 272 *Jan Ziekow/Corinna Sicko/Axel Piesker*, Abschied vom Arkanprinzip? Evaluation des Landesinformationsfreiheitsgesetzes Rheinland-Pfalz, Februar 2013.

Nr. 273 *Kai Masser*, Zwei Bürgerpanelbefragungen mit der Universitätsstadt Tübingen: 1. Wie finanzieren wir die Zukunft?“ 2010. 2, 2. „Kulturkonzeption der Universitätsstadt Tübingen“ 2011. Teil 2: Kulturkonzeption der Universitätsstadt Tübingen, Februar 2013.

Nr. 274 *Gisela Färber* unter Mitarbeit von *Marco Salm*, Gesetzesfolgenabschätzung unter der Genderperspektive – am Beispiel des Faktorverfahrens nach § 39f EStG, Gutachten im Auftrag des Bundesministeriums für Familie, Senioren, Frauen und Jugend (BMFSFJ), Juni 2013.

Nr. 275 *Kai Masser/Tobias Ritter/Jan Ziekow*, Erweiterte Bürgerbeteiligung bei Großprojekten in Baden-Württemberg – Abschätzung der Auswirkungen der Verwaltungsvorschrift „Bürgerdialog“ und des „Leitfadens für eine neue Planungskultur“ der Landesregierung, Mai 2014.

Nr. 276 *Gisela Färber/Marco Salm/Christian Schwab*, Evaluation des Verwaltungsmodernisierungsprozesses „CHANGE^2“ der Stadt Mannheim, Mai 2014.

Nr. 277 *Steffen Walther*, Reformen der Beamtenversorgung aus ökonomischer Perspektive, Juni 2014.

Nr. 278 *Stefan Preller*, Nachhaltige Finanzierung der Zusatzversorgung im öffentlichen Dienst, September 2014.

Nr. 279 *Joachim Wieland/Johanna Wolff*, Kommunales Vermögen – Kommunale Finanz- und Vermögensverwaltung unter Knappheitsbedingungen, Oktober 2014.

Nr. 280 *Mario Martini/Georg Thiel/Astrid Röttgen* (Hrsg.), Geodaten und Open Government – Perspektiven digitaler Staatlichkeit, November 2014.

Nr. 281 *María Jesús Montoro Chiner/Karl-Peter Sommermann* (Hrsg.), Gute Rechtsetzung – La Buena Legislación, März 2015.

Nr. 282 *Alexandra Lessau/Sarah Schmitt* (Hrsg.) im Auftrag Unterausschusses Allgemeine Verwaltungsorganisation des Arbeitskreises VI der Innenministerkonferenz, Aktivitäten auf dem Gebiet der Staats- und Verwaltungsmodernisierung in den Ländern und beim Bund 2011-2013, Juni 2015.

Nr. 283 *Jan Ziekow* (Hrsg.), Grenzgänge zwischen Wissenschaft und Praxis – Walking the Border between Theory and Practice, Forschungssymposium am 7. November 2014 zu Ehren von Eberhard Bohne zum 70. Geburtstag, November 2015.

Nr. 284 *Kai Masser/Franziska Fischer/Tobias Ritter,* Evaluation des Kommentieren-Bereichs des Beteiligungsportals des Landes Baden-Württemberg, November 2015.

Nr. 285 *Yukai WANG/Gisela FÄRBER* (ed.), Comparative Studies on Vertical Administrative Reforms in China and Germany, Juli 2016.

Nr. 286 *Mariá Jesús Montoro Chiner/Karl-Peter Sommermann* (Hrsg.), Soziale Rechte in Europa – Derechos sociales en Europa, September 2016.

Nr. 287 *Bernd W. Wirtz/Vincent Göttel/Marc-Julian Thomas/Paul F. Langer*, Bürgerorienterte WEB 2.0-Services – Eine empirische Anlalyse aus Bürgersicht, November 2016.

Nr. 288 *Kai Masser/Ingo Hamann/Jan Ziekow*, Evaluation, Verwaltungsvorschrift Öffentlichkeitsbeteiligung des Landes Baden-Württemberg. Analyse des Ressourcenaufwandes, Zwischenbilanz nach 1. Jahr Datenerhebung (2015), April 2017.

Nr. 289 *Michèle Morner/Manuel Misgeld/Markus Wojtczak*, Public Value durch E-Governance. Die Organisation kollaborativer Aktivitäten im Staat, Oktober 2017.

Nr. 290 *Jan Ziekow/Alfred G. Debus/Dieter Katz/Alexander Niestedt/Axel Piesker/Corinna Sicko*, Verdeckte Datenerhebungsmaßnahmen in der polizeilichen Praxis, Ergebnisse der Evaluation gemäß § 100 Polizei- und Ordnungsbehördengesetz Rheinland-Pfalz, März 2018.

Nr. 291 *Gisela Färber/Richard Hermanowski*, Entwicklungen des öffentlichen Dienstes seit der Deutschen Vereinigung und Forschungsbedarfe aus ökonomischer Perspektive, März 2018.

II. SELBSTÄNDIGE VERLAGSPUBLIKATIONEN

(nur im Buchhandel erhältlich)

250. *Jan Ziekow/Alfred G. Debus/Elisabeth Musch,* Bewährung und Fortentwicklung des Informationsfreiheitsrechts. Evaluierung des Informationsfreiheitsgesetzes des Bundes im Auftrag des Deutschen Bundestages, Schriften zur Evaluationsforschung, Bd. 1, Baden-Baden 2013.

251. *Jan Ziekow/Alfred G. Debus/Axel Piesker*, Die Planung und Durchführung von Gesetzesevaluationen. Ein Leitfaden unter besonderer Berücksichtigung datenschutzrechtlicher Eingriffe, Schriften zur Evaluationsforschung, Bd. 2, Baden-Baden 2013.

252. *Christoph Ewen/Oscar W. Gabriel/Jan Ziekow*, Bürgerdialog bei der Infrastrukturplanung: Erwartungen und Wirklichkeit. Was man aus dem Runden Tisch Pumpspeicherwerk Atdorf lernen kann, Schriften zur Evaluationsforschung, Bd. 3, Baden-Baden 2013.

253. *Jan Ziekow/Axel Piesker/Marco Salm/Corinna Sicko*, Neue Serviceangebote für Dienstleister. Erfahrungen mit den Einheitlichen Ansprechpartnern in Baden-Württemberg, Schriften zur Evaluationsforschung, Bd. 4, Baden-Baden 2014.

254. *Klaus König/Sabine Kropp/Sabine Kuhlmann/Christoph Reichard/Karl-Peter Sommermann/Jan Ziekow* (Hrsg.), Grundmuster der Verwaltungskultur. Interdisziplinäre Diskurse über kulturelle Grundformen der öffentlichen Verwaltung, Baden-Baden 2014.

255. *Christian Bauer,* Die Energieversorgung zwischen Regulierungs- und Gewährleistungsstaat. Die Gasnetzzugangs- und Gasnetzentgeltregulierung durch Bundesnetzagentur und Landesregulierungsbehörden, Schriftenreihe der Deutschen Universität für Verwaltungswissenschaften Speyer, Bd. 225, Berlin 2014.

256. *Insa Pruisken,* Fusionen im institutionellen Feld „Hochschule und Wissenschaft", Interdisziplinäre Schriften zur Wissenschaftsforschung Bd. 15, Baden-Baden 2014.

257. *Klaus König,* Operative Regierung, Tübingen 2015.

258. *Corinna Sicko/Dirk Zeitz/Jan Ziekow,* Neubau der sozialen Wohnraumförderung. Evaluierung des Landeswohnraumförderungsgesetzes Baden-Württemberg und Entwicklung von Regelungsperspektiven, Schriften zur Evaluationsforschung, Bd. 5, Baden-Baden 2015.

259. *Cristina Fraenkel-Haeberle/Sabine Kropp/Francesco Palermo/Karl-Peter Sommermann* (Hrsg.), Citizen Participation in Multi-Level Democracies, Leiden/Boston 2015.

260. *Bernd W. Wirtz,* E-Government – Perspektiven des kommunalen E-Government, Mainz 2015.

261. *Jürgen Kühling/Mario Martini/Johanna Heberlein/Benjamin Kühl/David Nink/Quirin Weinzierl/Michael Wenzel,* Die Datenschutz-Grundverordnung und das nationale Recht: Erste Überlegungen zum innerstaatlichen Regelungsbedarf, Berlin 2016.

262. *Jan Ziekow/Dieter Katz/Axel Piesker/Hanna Willwacher,* Gesetzliche Regelungen zur Terrorismusbekämpfung in Deutschland auf dem Prüfstand, Schriften zur Evaluationsforschung, Bd. 6, Baden-Baden 2016.

263. *Karl-Peter Sommermann* (Hrsg.), Öffentliche Angelegenheiten – interdisziplinär betrachtet. Forschungssymposium zu Ehren von Klaus König, Schriftenreihe der Deutschen Universität für Verwaltungswissenschaften Speyer, Bd. 230, Berlin 2016.

264. *Nadja Braun Binder*, Rechtsangleichung in der EU im Bereich der direkten Steuern. Analyse der Handlungsformen unter besonderer Berücksichtigung des Soft Law, Jus Publicum, Beiträge zum Öffentlichen Recht, Bd. 266, Tübingen 2017.

265. *Cristina Fraenkel-Haeberle/Diana-Urania Galetta/Karl-Peter Sommermann* (Hrsg.), Europäisierung und Internationalisierung der nationalen Verwaltungen im Vergleich - Deutsch-italienische Analysen, Schriften zum Europäischen Recht, Bd. 178, Berlin 2017.

266. *Benjamin Kühl*, Staatlich finanzierte Bewertungsportale Privater - Lebensmittelklarheit.de aus lebensmittel- und verfassungsrechtlicher Perspektive, Schriftenreihe der Wissenschaftlichen Gesellschaft für Lebensmittel

267. *Margrit Seckelmann/Johannes Platz* (Hrsg.), Remigration und Demokratie in der Bundesrepublik nach 1945. Ordnungsvorstellungen zu Staat und Verwaltung im transatlantischen Transfer, Histoire, Bd. 116, Bielefeld 2017.

268. *Jan Ziekow/Dieter Katz/Axel Piesker/Hanna Willwacher*, Die Rechtsextremismus-Datei in der polizeili-chen und nachrichtendienstlichen Praxis. Ergebnisse der Evaluation nach Artikel 3 Absatz 2 des Geset-zes zur Verbesserung der Bekämpfung des Rechtsextremismus, Schriften zur Evaluationsforschung, Bd. 7, Baden-Baden 2017.

269. *Veith Mehde/Margrit Seckelmann* (Hrsg.), Zum Zustand der repräsentativen Demokratie, Beiträge des Symposiums anlässlich des 80. Geburtstags von Hans Peter Bull, Tübingen 2017.

270. *Kai Masser/Bettina Engewald/Lucia Scharpf/Jan Ziekow*, Die Entwicklung der Mediation in Deutsch-land. Bestandsaufnahme nach fünf Jahren Mediationsgesetz, Schriften zur Evaluationsforschung, Bd. 8, Baden-Baden 2018.echt, Bd. 1,Frankfurt a.M.2017.

III. FÖV DISCUSSION PAPERS

(institutseigene Reihe, über das Institut zu beziehen)

Nr. 59 *Eberhard Bohne,* Clash of Regulatory Cultures in the EU: The Liberalization of Energy Markets , Speyer, Juni 2010.

Nr. 60 *Andreas Knorr/Jörg Bellmann/Rahel Schomaker,* International Trade Rules and Aircraft Manufacturing: Will the World Trade Organization Resolve the Airbus-Boeing Dispute?, Speyer, September 2010.

Nr. 61 *Albrecht Blümel/Katharina Kloke/Georg Krücken*, Hochschulkanzler in Deutschland: Ergebnisse einer hochschulübergreifenden Befragung, Speyer, September 2010.

Nr. 62 *Jonas Buche,* Die Europäisierung von Parteien und Parteisystemen - Eine Analyse am Beispiel Schwedens vom Beitritt zur EU 1995 bis zur Reichstagswahl 2006, Speyer, September 2010.

Nr. 63 *Andreas Knorr/Andreas Lueg-Arndt/Barbara Lueg*, Airport Noise Abatement as an International Coordination Problem – The Case of Zurich Airport, Februar 2011.

Nr. 64 *Gisela Färber*, Steuerhoheit von Gebietskörperschaften, März 2011.

Nr. 65 *Bernd W. Wirtz/Linda Mory/Robert Piehler*, Kommunales E-Government: Erfolgsfaktoren der Interaktion zwischen Stadtportalen und Anspruchsgruppen, März 2011.

Nr. 66 *Aron Buzogány/Andrej Stuchlik*, Paved with good intentions Ambiguities of empowering parliaments after Lisbon, Mai 2011.

Nr. 67 *Dennis Kutting*, Staatliche Verwaltungsarchitektur der 1950er Jahre in der Bundesrepublik, Forschungsstand, Problemstellung und Perspektiven, Juli 2011.

Nr. 68 *Ulrich Stelkens*, Art. 291 AEUV, das Unionsverwaltungsrecht und die Verwaltungsautonomie der Mitgliedstaaten, August 2011.

Nr. 69 *Gisela Färber*, Impacts of the Global Financial Crisis in a Federation: Evidence from Germany, Januar 2012.

Nr. 70 *Ulrich Stelkens/Hanna Schröder*, EU Public Contracts – Contracts passed by EU Institutions in Administrative Matters, März 2012.

Nr. 71 *Hans Herbert von Arnim*, Der Bundespräsident – Kritik des Wahlverfahrens und des finanziellen Status, März 2012.

Nr. 72 *Andreas Knorr*, Emissionshandel und Luftverkehr – Eine kritische Analyse am Beispiel des Europäischen Emissionshandelssystems (EU ETS) –, September 2012.

Nr. 73 *Gisela Färber/Julia Einsiedler*, Bürokratiekostenabbau im Steuerrecht: Ein Ansatz zur Vereinfachung des Steuerrechts? September 2012.

Nr. 74 *Tim Jäkel*, Wer vergleicht seine Leistung, wenn er hohe Schulden hat? Empirische Evidenz aus den deutschen kreisfreien Städten, Mai 2013.

Nr. 75 *Holger Mühlenkamp*, From State to Market Revisited: More Empirical Evidence on the Efficiency of Public (and Privately-owned) Enterprises, Juli 2013.

Nr. 76 *Dirk Zeitz*, Bewertung der Einfacher-zu-Projekte unter dem Blickwinkel eines Vollzugsbenchmarking, September 2013.

Nr. 77 *Stefan Domonkos*, Making Increased Retirement Age Acceptable: The Impact of Institutional Environment on Public Preferences for Pension Reforms, Juni 2014.

Nr. 78 *Daniela Caterina*, Construing and managing the crisis: A cultural political economy perspective on the Italian Labour Market Reform 2012, Juni 2014.

Nr. 79 *Marco Salm*, Property Taxes in BRICS: Comparison and a First Draft for Performance Measurement, Oktober 2014.

Nr. 80 *Dirk Zeitz,* Der Antrag auf Wohngeld als Beispiel der Konsequenzen des Exekutivföderalismus auf den Erfüllungsaufwand, April 2015.

Nr. 81 *Marco Salm/Christian Schwab,* HRM and Change Management: Comparative Results from Three European Cities of Excellence, November 2015.

Nr. 82 *Marius Herr,* Das E-Government-Gesetz des Bundes – Ein verwaltungswissenschaftlicher Literaturbericht –, November 2015.

Nr. 83 *Rahel M. Schomaker/Michael W. Bauer,* Experiments in Public Administration – some research, but no agenda, Juli 2016.

Nr. 84 *Dirk Zeitz,* Erprobung des Vollzugsbenchmarkings am Beispiel des Wohngeldes: Auswertung der Erhebungen, September 2016.

Nr. 85 *Mario Martini* unter Mitarbeit von *Saskia Fritzsche* und *Michael Kolain*, Digitalisierung als Herausforderung und Chance für Staat und Verwaltung. Forschungskonzept des Programmbereichs „Transformation des Staates in Zeiten der Digitalisierung“, Dezember 2016.

Nr. 86 *Ulrich Stelkens/Agne Andrijauskaite*, Added Value of the Council of Europe to Administrative Law: The Development of Pan-European General Principles of Good Administration by the Council of Europe and their Impact on the Administrative Law of its Member States. August 2017.

IV. Vorträge aus dem Deutschen Forschungsinstitut für öffentliche Verwaltung Speyer

(institutseigene Reihe, über das Institut zu beziehen)

Nr. 1 *Hans Peter Bull*, Vom Auf- und Abbau der Bürokratie, Januar 2006.

Nr. 2 *Janbernd Oebbecke,* Rechtswissenschaftliche Forschung und Verwaltung, Januar 2006.