Max-Planck-Institut
für ausländisches und
internationales Strafrecht

# Recht und Praxis der anlassbezogenen automatischen Kennzeichenfahndung, Verkehrsdatenabfrage und Mobilfunkortung zur Gefahrenabwehr in Brandenburg

Wissenschaftliche Begleitforschung zu den
§§ 33b Abs. 3, Abs. 6 Satz 2 und 36a BbgPolG

# Gutachten

der kriminologischen Abteilung des
Max-Planck-Instituts für ausländisches
und internationales Strafrecht

im Auftrag des Brandenburgischen Ministeriums des Innern

*Dr. Michael Kilchling*
*Brigitte Kenzel*

**Freiburg i.Br., April 2011**

**Hinweis zu Gender Mainstreaming:**

**Zur leichteren Lesbarkeit der Texte wurde die männliche Form von personenbezogenen Hauptwörtern gewählt. Eine Benachteiligung des weiblichen Geschlechts ist damit nicht beabsichtigt.**

## Vorbemerkungen

Das vorliegende Gutachten wurde im Auftrag des Brandenburgischen Ministeriums des Innern erstellt, der auf einen Beschluss des Landtags vom 17. Dezember 2008 zurückgeht. Die Evaluation soll eine wissenschaftliche Handreichung für die bevorstehende Neuregelung des Brandenburgischen Polizeigesetzes sein.

Die kriminologische Abteilung des Freiburger Max-Planck-Instituts für ausländisches und internationales Strafrecht hat seit einigen Jahren einen besonderen Forschungsschwerpunkt zur empirischen Strafverfahrensforschung. In diesem Kontext wurden bereits mehrere Forschungsprojekte zur Überwachung der Telekommunikation und zur Verkehrsdatenüberwachung sowie zu anderen besonderen Ermittlungsmaßnahmen wie der akustischen Wohnraumüberwachung und der Rasterfahndung durchgeführt. Des Weiteren wird derzeit im Auftrag des Bundesamtes für Justiz eine Untersuchung zu möglichen Schutzlücken durch den Wegfall der Vorratsdatenspeicherung erarbeitet. Der vorliegende Gutachtenauftrag ergänzt diese Forschungslinie auf sinnvolle Weise, da hier unter anderem die präventive Einsatzvariante der Verkehrsdatenabfrage zu untersuchen war. Die Forschungsarbeit war für die Bearbeiter damit weit mehr als ein zufälliger 'Ausflug' in das Polizei- und Ordnungsrecht. Die Untersuchung zeigt, dass solche Maßnahmen heute nicht mehr isoliert betrachtet werden können, weder aus der Perspektive des Polizeirechts noch aus der des Strafprozessrechts. Das zeigt gerade auch die Einsatzpraxis bei der anlassbezogenen automatischen Kennzeichenfahndung in Brandenburg.

Die Kennzeichenfahndung wird in dem vorliegenden Gutachten etwas ausführlicher behandelt als die anderen Maßnahmen. Dies ist der relativen Neuheit der Materie geschuldet. Während Fragen der Verkehrsdatenabfrage in den letzten Jahren in Literatur und Rechtsprechung sehr ausgiebig behandelt wurden, harren zahlreiche Fragestellungen im Bereich der Kennzeichenfahndung noch der endgültigen Klärung. Das Gutachten ist die erste systematische empirische Analyse in diesem Bereich.

Besonderen Dank schulden die Bearbeiter dem Brandenburgischen Ministerium des Innern, namentlich Herrn Regierungsdirektor Gerner, für die sehr gute Kooperation. Großer Dank gebührt auch den Mitarbeiterinnen und Mitarbeitern der beteiligten Polizeidienststellen, insbesondere Herrn Kriminalhauptkommissar Selchow, Fachkoordinator Kennzeichenfahndung, der stets ein offenes Ohr auch für kurzfristige telefonische Anfragen hatte.

Freiburg i.Br., 31.3.2011

Dr. Michael Kilchling

# Inhaltsverzeichnis

**Teil A: Einleitung** ..... **17**
1. Einführung ..... 17
2. Deskription der einzelnen Maßnahmen ..... 19
*2.1 Verkehrsdatenabfrage* ..... *19*
*2.2 Ortung von Mobiltelefonen* ..... *21*
*2.3 Anlassbezogene automatische Kennzeichenfahndung* ..... *22*
*2.4 Exkurs: An der Schnittstelle zwischen präventivem und repressivem Einsatz: Die Doppelfunktionalität polizeilichen Handelns* ..... *31*
**Teil B: Nationaler Rechtsvergleich** ..... **33**
1. Einleitung ..... 33
2. Verkehrsdatenabfrage ..... 34
*2.1 Brandenburg* ..... 34
*2.2 Baden-Württemberg* ..... 34
*2.3 Bayern* ..... 35
*2.4 Hamburg* ..... 36
*2.5 Hessen* ..... 37
*2.6 Mecklenburg-Vorpommern* ..... 37
*2.7 Niedersachsen* ..... 38
*2.8 Rheinland-Pfalz* ..... 38
*2.9 Saarland* ..... 38
*2.10 Schleswig-Holstein* ..... 39
*2.11 Thüringen* ..... 40
*2.12 Andere Bundesländer* ..... 40
*2.13 Zusammenfassung* ..... 40
3. Ortung von Mobiltelefonen ..... 41
*3.1 Brandenburg* ..... 42
*3.2 Baden-Württemberg* ..... 42
*3.3 Bayern* ..... 43
*3.4 Berlin* ..... 43
*3.5 Bremen* ..... 44
*3.6 Hamburg* ..... 44
*3.7 Hessen* ..... 45
*3.8 Mecklenburg-Vorpommern* ..... 45

*3.9 Niedersachsen* ..... 45
*3.10 Rheinland-Pfalz* ..... 46
*3.11 Saarland* ..... 47
*3.12 Schleswig-Holstein* ..... 48
*3.13 Thüringen* ..... 48
*3.14 Andere Bundesländer* ..... 49
*3.15 Zusammenfassung* ..... 49
4. Automatische Kennzeichenfahndung ..... 49
*4.1 Brandenburg* ..... 50
*4.2 Baden-Württemberg* ..... 50
*4.3 Bayern* ..... 52
*4.4 Hamburg* ..... 53
*4.5 Hessen* ..... 53
*4.6 Mecklenburg-Vorpommern* ..... 54
*4.7 Niedersachsen* ..... 55
*4.8 Rheinland-Pfalz* ..... 55
*4.9 Saarland* ..... 56
*4.10 Schleswig-Holstein* ..... 56
*4.11 Thüringen* ..... 57
*4.12 Andere Bundesländer* ..... 57
*4.13 Zusammenfassung* ..... 58
**Teil C: Internationaler Rechtsvergleich** ..... **73**
1. England & Wales ..... 73
*1.1 Verkehrsdatenabfrage und Ortung von Mobiltelefonen* ..... *73*
*1.2 Automatische Kennzeichenfahndung* ..... *74*
2. Finnland ..... 75
*2.1 Verkehrsdatenabfrage und Ortung von Mobiltelefonen* ..... *75*
*2.2 Automatische Kennzeichenfahndung* ..... *75*
3. Frankreich ..... 76
*3.1 Verkehrsdatenabfrage und Ortung von Mobiltelefonen* ..... *76*
*3.2 Automatische Kennzeichenfahndung* ..... *77*
4. Österreich ..... 77
*4.1 Verkehrsdatenabfrage und Ortung von Mobiltelefonen* ..... *78*
*4.2 Automatische Kennzeichenfahndung* ..... *79*
5. Polen ..... 79
*5.1 Verkehrsdatenabfrage und Ortung von Mobiltelefonen* ..... *79*
*5.2 Automatische Kennzeichenfahndung* ..... *80*
6. Schweden ..... 80

*6.1 Verkehrsdatenabfrage und Ortung von Mobiltelefonen ..... 81*
*6.2 Automatische Kennzeichenfahndung ..... 82*
7. Schweiz ..... 82
*7.1 Verkehrsdatenabfrage und Ortung von Mobiltelefonen ..... 83*
*7.2 Automatische Kennzeichenfahndung ..... 85*
8. Tschechien ..... 86
*8.1 Verkehrsdatenabfrage und Ortung von Mobiltelefonen ..... 87*
*8.2 Automatische Kennzeichenfahndung ..... 87*
9. Ungarn ..... 87
*9.1 Verkehrsdatenabfrage und Ortung von Mobiltelefonen ..... 87*
*9.2 Automatische Kennzeichenfahndung ..... 87*
10. Zusammenfassung ..... 88

**Teil D: Rechtliche Bewertung der brandenburgischen Regelungen ..... 89**
1. Verkehrsdatenabfrage ..... 89
2. Ortung von Mobiltelefonen ..... 95
3. Anlassbezogene automatische Kennzeichenfahndung ..... 95

**Teil E: Anwendungspraxis in Brandenburg ..... 112**
1. Einleitung ..... 112
2. Verkehrsdatenabfrage und Ortung von Mobiltelefonen ..... 112
3. Anlassbezogene automatische Kennzeichenfahndung ..... 129

**Teil F: Abschließende Bewertung und Empfehlungen ..... 153**
1. Allgemeines ..... 153
2. Verkehrsdatenabfrage und Ortung von Mobiltelefonen ..... 153
3. Anlassbezogene automatische Kennzeichenfahndung ..... 155
4. Formulierungsvorschläge ..... 156

**Teil G: Anhänge**
1. Aktuelle Gesetzestexte ..... 161
*§ 33b BbgPolG ..... 161*
*§ 36a BbgPolG ..... 163*
2. Expertengespräche ..... 164
3. Variablenplan ..... 175
4. Erlass vom 14.7.2010 ..... 182

# Verzeichnis der Abbildungen, Übersichten, Tabellen und Schaubilder

Abbildung 1: Stationäres Kamerasystem ..... 24
Abbildung 2a: Trefferbild 1 ..... 25
Abbildung 2b: Trefferbild 2 ..... 26

Übersicht 1: Regelungen zur Verkehrsdatenabfrage in den Bundesländern ..... 60
Übersicht 2: Regelungen zur Standortbestimmung in den Bundesländern ..... 64
Übersicht 3: Regelungen zur automatischen Kennzeichenfahndung in den Bundesländern ..... 68
Übersicht 4: Kfz-Diebstahl in Deutschland gem. Polizeilicher Kriminalstatistik ..... 107
Übersicht 5: Einige exemplarische Sachverhalte bei der Verkehrsdatenabfrage ..... 120

Tabelle 1: Häufigkeit der Verkehrsdatenabfrage und Mobilfunkortung ..... 112
Tabelle 2: VDA-Einsatzzahlen im zeitlichen Verlauf (1.1.2009 bis 30.6.2010) ..... 113
Tabelle 3: VDA-Einsatzzahlen in Relation zu der Gesamtzahl der präventiven Maßnahmen ..... 115
Tabelle 4: Anzahl gefährdeter Personen ..... 119
Tabelle 5: Anordnende Behörde ..... 122
Tabelle 6: Anzahl betroffener Mobilanschlüsse ..... 122
Tabelle 7: Zielpersonen der Verkehrsdatenabfrage ..... 125
Tabelle 8: Beauskunftung durch die Telekommunikationsunternehmen ..... 125
Tabelle 9: Anzahl der präventiven Verkehrsdatenzugriffe in Brandenburg für jeden Tag des Evaluationszeitraumes ..... 126
Tabelle 10: Fallzahlen der Automatischen Kennzeichenfahndung und polizeiliche Einsätze insgesamt (2009 und 2010) ..... 129
Tabelle 11: Automatische Kennzeichenfahndung – Anwendungshäufigkeit im Evaluationszeitraum (Jan. 2009 bis Sept. 2010) ..... 130
Tabelle 12: Entwicklung der AKF in Relation zu der Gesamtzahl polizeilicher Einsätze ..... 132
Tabelle 13: Art der eingesetzten Systeme ..... 133
Tabelle 14: Einsatzmodus der Systeme ..... 135
Tabelle 15: Anordnung der Maßnahmen ..... 135
Tabelle 16: Anlass der Kennzeichenfahndung ..... 136
Tabelle 17: Zielsetzung der Kennzeichenfahndung ..... 138
Tabelle 18: Anzahl überwachter Kfz-Kennzeichen nach Fallgruppen ..... 139
Tabelle 19: Anzahl eingesetzter Systeme ..... 141
Tabelle 20: Durchschnittliche Anzahl eingesetzter Systeme ..... 143
Tabelle 21: Dauer der Fahndungsmaßnahmen ..... 144

Tabelle 22: Treffermeldungen ..... 146
Tabelle 23: Aktiver Fahndungsbestand bei der AKF in Brandenburg für jeden Tag des Evaluationszeitraumes ..... 147

Schaubild 1: Entwicklung der VDA-Einsatzzahlen absolut im zeitlichen Verlauf ..... 114
Schaubild 2a: Entwicklung der VDA-Einsatzzahlen und der präventiven Maßnahmen insgesamt ..... 116
Schaubild 2b: Entwicklung der VDA-Einsatzzahlen und der präventiven Maßnahmen insgesamt (2) ..... 116
Schaubild 3a: Repressive und präventive VDA in Brandenburg (2009) ..... 117
Schaubild 3b: Repressive und präventive VDA in Brandenburg (Januar bis Juni 2010) ..... 118
Schaubild 4: Anzahl gefährdeter Personen (2) ..... 119
Schaubild 5: Zielpersonen der Verkehrsdatenabfrage (2) ..... 123
Schaubild 6: Beauskunftung durch die Telekommunikationsunternehmen (2) ..... 125
Schaubild 7: Entwicklung der Automatischen Kennzeichenfahndung absolut im zeitlichen Verlauf ..... 131
Schaubild 8: Entwicklung der AKF-Einsatzzahlen und der polizeilichen Einsätze insgesamt ..... 133
Schaubild 9: Art der eingesetzten Systeme (2) ..... 134
Schaubild 10: Anlass der Kennzeichenfahndung (2) ..... 137
Schaubild 11: Zielsetzung der Kennzeichenfahndung (2) ..... 138
Schaubild 12: Durchschnittliche Anzahl eingesetzter Systeme im Zeitverlauf ..... 142
Schaubild 13: Dauer der Fahndungsmaßnahmen ..... 145

## Literaturverzeichnis

Achenbach, H.: Vorläufige Festnahme, Identifizierung und Kontrollstelle im Strafprozess, JA 1981, 660.

Albrecht, H.-J. / Grafe, A. / Kilchling, M.: Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO. Kriminologische Forschungsberichte aus dem Max-Planck-Institut, Band K 139, Berlin 2008.

Albrecht, H.-J. / Dorsch, C. / Krüpe, C.: Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsarten. Freiburg im Breisgau 2003.

Arzt, C.: Polizeiliche Datenerhebung und Datenverarbeitung zur Gefahrenabwehr im Straßenverkehr. SVR 2006, 10.

Arzt, C.: Rechtsfragen der automatisierten Kennzeichenerkennung. SVR 2004, 321.

Arzt, C.: Voraussetzungen und Grenzen der automatisierten Kennzeichenerkennung. DÖV 2005, 56.

Bär, W.: Telekommunikationsüberwachung und andere verdeckte Ermittlungsmaßnahmen Gesetzliche Neuregelungen zum 1.1.2008. MMR 2008, 215.

Belz, R. / Mußmann, E.: Polizeigesetz Baden-Württemberg. 7. Auflage, Stuttgart 2009.

Beulke, W.: Strafprozessrecht. 11. Auflage, Heidelberg 2010.

Bodenbenner, D. / Heinemann, M.: Die Neuregelung der automatisierten Kennzeichenerfassung in Hessen. NVwZ 2010, 679.

Böhrenz, G. / Siefken, P.: Niedersächsisches Gesetz über die öffentliche Sicherheit und Ordnung. 9. Auflage, Hannover 2008.

Brandner, H. E.: Das allgemeine Persönlichkeitsrecht in der Entwicklung durch die Rechtsprechung. JZ 1983, 689.

Braun, F. / Seidl, A.: Verfassungsmäßigkeit des verdeckten Einsatzes automatisierter Kennzeichenerkennungssysteme im Polizeiaufgabengesetz Bayerns. jurisPR-ITR 13/2010 Anm. 6.

Breyer, P.: Die systematische Aufzeichnung und Vorhaltung von Telekommunikations-Verkehrsdaten für staatliche Zwecke in Deutschland. Berlin 2005.

Breyer, P.: Kfz-Massenabgleich nach dem Urteil des Bundesverfassungsgerichts. NVwZ 2008, 824.

Bücken, M.: Zulässige Aufzeichnung und Nutzung von Videoaufnahmen zur Verfolgung von Verkehrsordnungswidrigkeiten. jurisPR-VerkR 20/2010, Anm. 4.

Burghard, W.: Editorial: Aufgaben, Erwartungen und Handlungsbedingungen. Kriminalistik 1994, 227.

Corbett, C.: Techno-Surveillance of the Roads: High Impact and Low Interest. Crime Prevention and Community Safety 2008, 1.

Cornils, M.: Grundrechtsschutz gegenüber polizeilicher Kfz-Kennzeichenüberwachung. Jura 2010, 443.

Dorsch, C.: Die Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO, Berlin 2005.

Dreier, H.: Grundgesetz – Kommentar. 2. Auflage, Tübingen 2004.

Dreier, H.: Grundgesetz – Kommentar. Band 1. Tübingen 1996.

Ehrenberg, W. / Frohne, W.: Doppelfunktionale Maßnahmen der Vollzugspolizei – Problematik der rechtlichen Einordnung. Kriminalistik 2003, 737.

Eisenberg, U. / Singelnstein, T.: Zur Unzulässigkeit der heimlichen Ortung per „stiller SMS". NStZ 2005, 62.

Emmering, E.: Die Doppelfunktion der Polizei. DVBl. 1958, 338.

Erd, R.: Bundesverfassungsgericht versus Politik – Eine kommentierende Dokumentation der jüngsten Entscheidungen zu drei Sicherheitsgesetzen. KJ 2008, 118.

Frenz, W.: Informationelle Selbstbestimmung im Spiegel des BVerfG. DVBl 2009, 333.

Geppert, M. / Piepenbrock, H.-J. / Schütz, R. / Schuster, F. (Hrsg.): Beck'scher TKG-Kommentar. 3. Auflage, München 2006.

Götz, V.: Allgemeines Polizei- und Ordnungsrecht. 14. Auflage, München 2008.

Gras, M.: Kriminalprävention durch Videoüberwachung. Baden-Baden 2003.

Gusy, C.: Rasterfahndung nachPolizeirecht? KritV 2002, 474.

Hammerstein, C. von: Kostentragung für staatliche Überwachungsmaßnahmen nach der TKG-Novelle. MMR 2004, 222.

Hannich, R. (Hrsg): Karlsruher Kommentar zur Strafprozessordnung. 6. Auflage, München 2008.

Harnisch, S. / Pohlmann, M.: Strafprozessuale Maßnahmen bei Mobilfunkendgeräten – Die Befugnis zum Einsatz des sog. IMSI-Catchers. HRRS 2009, 202.

Hoffmann-Riem, W.: Freiheit und Sicherheit im Angesicht terroristischer Anschläge. ZRP 2002, 497.

Honess, T. / Charman, E.: Closed Circuit Television in Public Places. London 1992.

Hornmann, G.: Die Novellierung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung im Jahr 2009. NVwZ 2010, 292.

Hornmann, G.: Verfassungswidrigkeit der Befugnis über den automatisierten Kfz-Kennzeichenabgleich im Hessischen Polizeirecht. NVwZ 2007, 669.

Hudson, S.: Automatic number plate recognition. Magistrate 2008, H. 3, 68.

Kilchling, M.: Die Überwachung der Telekommunikation in Deutschland. Yenisey, F. / Sieber, U. (Hrsg.): Criminal Law in the Global Risk Society. Istanbul 2011, 613.

Kniesel, M.: Neue Polizeigesetze contra StPO? Zum Regelungsstandort der vorbeugenden Bekämpfung von Straftaten und zur Verfassungsmäßigkeit polizeilicher Vorfeldaktivitäten. ZRP 1987, 377.

Kotowski, W.: Ustawa o Policji. Komentarz. 2. Auflage, Warschau 2008.

Krasuski, A.: Prawo telekomunikacyjne. Komentarz. 3. Auflage, Warschau 2009.

Kube, H. / Schütze, M.: Die Kosten der TK-Überwachung. CR 2003, 663.

Kutscha, M.: Überwachungsmaßnahmen von Sicherheitsbehörden im Fokus der Grundrechte. LKV 2008, 481.

Lang, M.: Die polizeirechtlichen Grundlagen für den Einsatz von Videoüberwachungstechnik im öffentlichen Raum. JurPC Web-Dok. 93/2005, Abs. 1-100.

Leibholz, G. / Rinck H.J.: Grundgesetz für die Bundesrepublik Deutschland, Kommentar anhand der Rechtsprechung des BVerfG., 46. Auflage, Köln 2007.

Lisken, H.: „Verdachts- und ereignisunabhängige Personenkontrollen zur Bekämpfung der grenzüberschreitenden Kriminalität"? NVwZ 1998, 22.

Lloyd, I.: A Guide to the Data Protection Act 1998. London 1998.

Löffelmann, M.: Aktuelle Rechtsprobleme der Telekommunikationsüberwachung. AnwBl 2006, 598.

Löwe, E. / Rosenberg, W.: Die Strafprozessordnung und das Gerichtsverfassungsgesetz – Großkommentar, 2. Band. 25. Auflage, Berlin 2004 [zitiert: Löwe/Rosenberg-Bearbeiter].

Marx, G.: Seeing Hazily (But Not Darkly) Through the Lens – Some Recent Empirical Studies of Surveillance Technologies. Law & Social Inquiry 2006, 339.

Marx, G.: Soft Surveillance – Mandatory Voluntarism and the Collection of Personal Data. Dissent 2005, 36.

Maunz, T. / Dürig, G.: Grundgesetz – Kommentar. Band 1. München 2009.

McCahill, M. / Norris, C.: Estimating the Extent, Sophistication and Legality of CCTV in London. Gill, Martin (Hrsg.): CCTV. Leicester 2003.

Meyer-Goßner, L.: Strafprozessordnung. 53. Auflage, München 2010.

Meyer-Goßner, L.: Strafprozessordnung. 49. Auflage, München 2006.

Nachbaur, A.: Standortfeststellung und Art. 10 GG Artikel 10 GG – Der Kammerbeschluss des BVerfG zum Einsatz des „IMSI-Catchers". NJW 2007, S. 335.

Nolte, M.: Doppelfunktionale Maßnahmen in der polizeilichen Praxis. Kriminalistik 2007, 343.

Ortmann, R.: Sozialtherapie im Strafvollzug – Eine experimentelle Längsschnittstudie zu den Wirkungen von Strafvollzugsmaßnahmen auf Legal- und Sozialbewährung. Freiburg im Breisgau 2002.

Pawelec, K. J.: Prawo o ruchu drogowym. Komentarz. Warschau 2005.

Pehl, D.: Die Implementation der Rasterfahndung. Kriminologische Forschungsberichte aus dem Max-Planck-Institut, Band K 140, Berlin 2008.

Pfeifer, G. (Hrsg.): Karlsruher Kommentar zur Strafprozessordnung und zum Gerichtsverfassungsgesetz. 5. Auflage, München 2003. [zitiert: Bearbeiter, in: Karlsruher Kommentar]

Riegel, R.: Rechtsprobleme der Rasterfahndung. ZRP 1980, 300.

Robrecht, M. P.: Automatische Kennzeichenerkennung – eine zulässige Kompensation weggefallener Grenzkontrollen? NJ 2008, 9.

Roggan, F.: Das novellierte Brandenburgische Polizeigesetz. NJ 2007, 199.

Roggan, F.: Moderne Telekommunikationsüberwachung: Eine kritische Bestandsaufnahme. KritV 2003, 76.

Roßnagel, A.: Die „Überwachungs-Gesamtrechnung" – Das BVerfG und die Vorratsdatenspeicherung. NJW 2010, 1238.

Roßnagel, A.: Kennzeichenscanning – Umsetzung der Vorgaben des Bundesverfassungsgerichts. Kassel 2009.

Roßnagel, A.: Kennzeichenscanning – Verfassungsrechtliche Bewertung. München 2008.

Roßnagel, A.: Verdachtslose automatisierte Erfassung von Kfz-Kenzeichen. DAR 2008, 61.

Roßnagel, A.: Verfassungsrechtliche Grenzen polizeilicher Kfz-Kennzeichenerfassung. NJW 2008, 2547.

Rowe, H.: Tolley's Data Protection Act 1998 – A Practical Guide. Bath 2000.

Roxin, C. / Schünemann, B.: Strafverfahrensrecht. 26. Auflage, München 2009.

Ruder, K.-H. / Schmitt, S.: Polizeirecht Baden-Württemberg. 7. Auflage, Baden-Baden 2011.

Rudolphi, H.-J.: Systematischer Kommentar zur Strafprozessordnung und zum Gerichtsverfassungsgesetz. 50. Auflage, Frankfurt am Main 2006. [zitiert: Bearbeiter, in: SK]

Säcker, F.J. (Hrsg.): Berliner Kommentar zum Telekommunikationsgesetz. 2. Auflage, Frankfurt 2009.

Schenke, W.-R.: Polizei- und Ordnungsrecht. 6. Auflage, Heidelberg 2009.

Scheurle, K.-D., Mayen, T.: Telekommunikationsgesetz. Kommentar. 2. Auflage, München 2008.

Schieder, A.: Die automatisierte Erkennung amtlicher Kfz-Kennzeichen als polizeiliche Maßnahme. NVwZ 2004, 778.

Schmidt, V.: Handy-Ortung zur Gefahrenabwehr – Zur Rechtmäßigkeit von Auskunftsersuchen an Netzbetreiber. Kriminalistik 2002, 42.

Schmidt-Preuß, M.: Die verfassungsrechtlichen Anforderungen an die Entschädigung für Leistungen der Telekommunikationsüberwachung und der Auskunftserteilung. Kurzgutachten. Bonn 2005.

Schoreit, A.: Datenverarbeitung, Datenschutz und Strafrecht. DRiZ 1987, 82.

Schramm, M. / Wegener, D.: Neue Anforderungen an eine anlasslose Speicherung von Vorratsdaten. Umsetzungsmöglichkeiten der Vorgaben des Bundesverfassungsgerichts. MMR 2011, S. 9.

Schüler, R.: Das Automatische Kennzeichen Lese System (AKLS). PVT 2007, 1.

Sommer, U.: Die Zukunft der polizeilichen Überwachung. AnwBl 2006, 633.

Vogelgesang, K.: Grundrecht auf informationelle Selbstbestimmung? Göttingen 1986.

Volkmann, U.: Die Verabschiedung der Rasterfahndung als Mittel der vorbeugenden Verbrechensbekämpfung. Jura 2007, 132.

Vollmar, T. J.: Telefonüberwachung im Polizeirecht. Frankfurt 2008.

Welp, J.: Überwachung und Kontrolle, Berlin 2000.

Weßlau, E.: Gefährdung des Datenschutzes durch den Einsatz neuer Medien im Strafprozess. ZStW 2003, 681.

Wolf, H. / Stephan, U. / Deger, J.: Polizeigesetz für Baden-Württemberg. 6. Auflage, Stuttgart 2009.

Würtenberger, T. / Heckmann, D.: Polizeirecht in Baden-Württemberg. 6. Auflage, Heidelberg 2005.

Zöller, M. A.: Möglichkeiten und Grenzen polizeilicher Videoüberwachung. NVwZ 2005, 1235.

# Teil A: Einleitung

## 1. Einführung

### *1.1 Fragestellung*

Die vorliegende Untersuchung geht auf einen Beschluss des Landtages Brandenburg vom 17. Dezember 2008[1] zurück. Danach sollten verschiedene Maßnahmen des Brandenburgischen Polizeigesetzes wissenschaftlich evaluiert werden. Dies betrifft die präventive Verkehrsdatenabfrage gem. § 33b Abs. 6 S. 2 BbgPolG, die Ortung von Mobiltelefonen gem. § 33b Abs. 3 Nr. 2 BbgPolG sowie die anlassbezogene automatische Kennzeichenfahndung gem. § 36a BbgPolG. Analysiert werden sollten unter anderem die Erhebungspraxis, der Nutzen der gewonnenen Daten für die polizeiliche Arbeit sowie die Effektivität und Effizienz der verdeckten Datenerhebungen, auch in Kombination mit anderen Befugnissen. Dabei sollten insbesondere Anlass, Umfang, Dauer, Ergebnis, Anzahl der Betroffenen und die Wirkung der Befugnisse berücksichtigt sowie rechtliche und praktische Anwendungsprobleme erforscht und eventuelle Verbesserungsvorschläge erarbeitet werden.

### *1.2 Anlage der Untersuchung*

#### *1.2.1 Methodische Erwägungen*

Ausgangspunkt und inhaltlicher Referenzrahmen der vorliegenden Untersuchung sind die genannten Bestimmungen des BbgPolG. Mit in die Bewertung einfließen müssen aber das gesamte Normengefüge des Brandenburgischen Polizeigesetzes, die Komplementärvorschriften der StPO, die telekommunikationsrelevanten Rahmenbestimmungen des TKG sowie die verfassungsrechtlichen Rahmenbedingungen. Diese weite Perspektive erscheint besonders im Hinblick auf die Doppelfunktion der Polizei als Behörde zur Gefahrenabwehr und als Ermittlungsorgan der Staatsanwaltschaft mit den in den §§ 163ff. StPO vorgesehenen Befugnissen essentiell.[2] Die fraglichen Maßnahmen ausschließlich in ihrer präventiven Funktion zu beurteilen, würde der Komplexität moderner Sicherheitsgesetzgebung nicht gerecht. Dies zeigt sich im Rahmen dieser Evaluation exemplarisch am Beispiel des Kfz-Diebstahls, der in Brandenburg mit weitem Abstand den Hauptanwendungsbereich der automatischen Kennzeichenfahndung ausmacht.

Darüber hinausreichende Implikationen durch verbindliche Rechtsakte der Europäischen Union wurden zwar geprüft. Mangels einschlägiger Vorgaben für die hier zu untersuchenden besonderen polizeirechtlichen Eingriffsbefugnisse auf der Ebene eines Bundeslandes wird dieser Aspekt in dem Gutachten nicht näher behandelt.

Die Untersuchung hat zwei Hauptaspekte: die Analyse der aktuellen rechtlichen Regelungen zu den drei Maßnahmen sowie die Evaluation der Anwendungspraxis.

---

[1] Drucksache 4/7008-B.

[2] Siehe dazu auch die Ausführungen gleich unter Pkt. 2.3.4.

Neben der rechtlichen Würdigung der genannten Rechtsgrundlagen (Teil D) und der empirischen Analyse ihrer Anwendung (Teil E) wurden ergänzend zwei rechtsvergleichende Abschnitte erarbeitet. Der eine präsentiert einen systematischen Vergleich der Rechtslage im Hinblick auf die drei hier zu untersuchenden Maßnahmen in den anderen Bundesländern (Teil B). Der andere gibt einen Überblick über die Situation in einigen ausgewählten europäischen Rechtsordnungen (Teil C). Eine kurze Würdigung und einige rechtspolitische Empfehlungen schließen die Untersuchung ab (Teil F).

### *1.2.2 Datenzugänge*

Die Informationen und Daten, auf denen die Untersuchungsergebnisse basieren, wurden aus unterschiedlichen Quellen generiert.

Alle wesentlichen Informationen, die die Organisation und Einsatzpraxis betreffen, wurden auf der Grundlage von persönlichen Interviews mit Polizeipraktikern verschiedener Behörden gewonnen. Die Interviews wurden zu zwei unterschiedlichen Zeitpunkten durchgeführt. Ein erstes Modul am Beginn der Projektlaufzeit diente der Klärung aller relevanten inhaltlichen Fragen[3]. Ein zweites, späteres Modul diente vor allem der Klärung einzelner technischer Nachfragen zu den bis dahin gesammelten Evaluationsdaten.

Alle einschlägigen Fälle aus dem Evaluationszeitraum wurden auf der Basis eines Erlasses des Ministerium des Innern zur Umsetzung des Landtagsbeschlusses von den zuständigen Polizeibehörden mit einigen wesentlichen Grundinformationen in Excel-Listen erfasst und in mehreren Tranchen an das Max-Planck-Institut übermittelt. Sie bildeten die Basis für die statistische Erfassung in einer SPSS-fähigen Falldatei[4].

Für alle einschlägigen Fälle wurden sodann, soweit vorhanden, die zugehörigen polizeilichen Akten bzw. sonstigen Dokumentationen und Aufzeichnungen angefordert und ausgewertet.[5] Die hierbei gewonnen Daten bilden das Kernstück der empirischen Analyse (Teil E). Es handelt sich dabei um eine Vollerhebung. Anders als ursprünglich geplant konnte keine ausreichende Zahl zugehöriger Justizakten identifiziert werden, sodass verlässliche Aussagen über mögliche strafrechtliche Konsequenzen, die zumindest für einige – wenn auch nur wenige – der von den polizeilichen Maßnahmen Betroffenen eingetreten sein könnten. Freilich würde dieser Aspekt die Frage der Rechtmäßigkeit der polizeilichen Maßnahmen nicht tangieren.

Ergänzend wurden schließlich weitere statistische Informationen in die Analyse einbezogen. Dies betrifft insbesondere die erforderlichen Vergleichsdaten über das generelle Fallaufkommen und seine Verteilung bei der brandenburgischen Polizei. Hierfür wurden Daten aus dem elektronischen Einsatzleit- und Erfassungssystem ELBOS[6] herangezogen.

---

[3] Siehe Teil G, Anhang 2.

[4] Bei SPSS handelt es sich um die im Bereich der empirischen Sozialforschung meist verwendete Statistik- und Analysesoftware („Statistical Package for the Social Sciences").

[5] Siehe hierzu den Variablenplan in Teil G, Anhang 3.

[6] Siehe hierzu die Ausführungen in Teil E zu den Tabellen 3.

*1.2.3 Evaluationszeitraum*

Aus forschungstechnischen Gründen wurden die Maßnahmen in unterschiedlichen Zeiträumen evaluiert. Der Grund hierfür liegt in der zeitaufwendigen Identifikation, Sammlung und Auswertung der sehr viel umfangreicheren Akten zu den verkehrsdatenbezogenen Maßnahmen. Daher wurde für die Untersuchung der Maßnahmen gem. § 33b BbgPolG ein etwas kürzerer Zeitraum vom 18 Monaten gewählt. In die Evaluation eingeflossen sind alle Maßnahmen vom 1.1.2009 bis zum 30.6.2010.

Die Informationen zu den Maßnahmen gem. § 36a BbgPolG waren hingegen leichter zu ermitteln und weniger umfangreich. Daher konnten auch noch alle Maßnahmen aus dem dritten Quartal 2010 in die Analyse einfließen. Damit sind hier sämtliche Maßnahmen berücksichtigt, die vom 1.1.2009 bis zum 30.9.2010 durchgeführt wurden.

In zwei Zwischenberichten zum 7.12.2009 und 7.12.2010 wurde dem Ministerium des Innern über den Fortgang der Projektarbeiten Bericht erstattet.

## 2. Deskription der einzelnen Maßnahmen

### *2.1 Verkehrsdatenabfrage gem. § 33b Abs. 6 S. 2 BbgPolG*

§ 33b Abs. 6 S. 2 BbgPolG erlaubt den Zugriff auf vorhandene und künftige Verkehrsdaten einschließlich der für die Ermittlung des Standortes eines Mobilfunkendgerätes erforderlichen spezifischen Kennungen, insbesondere die Geräte- und Kartennummer sowie die Zellinformationen. Die Vorschrift ist eine reine Zugriffsnorm. Adressat sind die Telekommunikationsanbieter, die die Daten vorhalten und verpflichtet sind, der Polizei auf Anfrage die benötigten Auskünfte zu erteilen. Die Speicherpflichten selbst ergeben sich nicht aus dem Landesrecht, sondern sind im Telekommunikationsgesetz (TKG[7]) geregelt.

*2.1.1 Definition*

Der Begriff Verkehrsdaten wird in § 3 Nr. 30 TKG legal definiert. Es handelt sich danach um Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden. Früher wurde in einigen Gesetzen fast synonym auch der Begriff der „Verbindungsdaten" verwandt.[8] Dieser Begriff ist inzwischen weitgehend gestrichen und durch die neue Terminologie ersetzt worden. Standortdaten sind nach § 3 Nr. 19 TKG die in einem Telekommunikationsnetz erhobenen oder verwendeten Daten, die den Standort eines Endgeräts angeben. Es handelt sich also um geographische Positionsangaben, die u.a. Aufschluss über den aktuellen Standort des Gerätes und damit möglicherweise auch seines Trägers geben können. Das macht die besondere Bedeutung dieser Datenart für Zwecke der Gefahrenabwehr aus. Genaugenommen handelt es sich um einen Unterfall von Verkehrsdaten.

---

[7] Telekommunikationsgesetz v. 22.06.2004, BGBl. I S. 1190, zuletzt geändert durch Artikel 3 des Gesetzes v. 24.03.2011, BGBl. I S. 506. Die wesentlichen Änderungen der letzten Jahre sind übersichtlich nachgezeichnet bei www.buzer.de/gesetz/6833/l.htm

[8] Vgl. näher *Albrecht/Grafe/Kilchling* 2008.

Streng zu unterscheiden ist die Verkehrsdatenabfrage von der Telekommunikationsüberwachung im klassischen Sinne, die auch auf die Inhalte der Kommunikation zugreift.[9]

### *2.1.2 Speicherung*

Allgemeine Telekommunikationsverkehrsdaten dürfen grundsätzlich nach § 96 TKG erhoben werden. Diese Ermächtigung richtet sich an die Telekommunikationsanbieter und umfasst die folgenden Verkehrsdaten:

- die Nummer oder Kennung der beteiligten Anschlüsse oder der Endeinrichtung, personenbezogene Berechtigungskennungen, bei Verwendung von Kundenkarten auch die Kartennummer, bei mobilen Anschlüssen auch die Standortdaten,
- der Beginn und das Ende der jeweiligen Verbindung,
- die übermittelten Datenmengen, soweit die Entgelte davon abhängen,
- der vom Nutzer in Anspruch genommene Telekommunikationsdienst,
- die Endpunkte von festgeschalteten Verbindungen, ihren Beginn und ihr Ende und – soweit Entgelte davon abhängen – die übermittelten Datenmengen,
- sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendige Verkehrsdaten.

Nach § 96 Abs. 2 ist eine über Abs. 1 hinausgehende Erhebung oder Verwendung von Verkehrsdaten ausdrücklich unzulässig. Der primäre Zweck der allgemeinen Verkehrsdaten liegt nach den §§ 96, 97 TKG zum einen in der Ermöglichung eines technisch korrekten Verbindungsaufbaus und – vor allem – in der Schaffung der notwendigen Grundlagen für eine korrekte Entgeltermittlung und -abrechnung. Dem Anbieter wird in diesem Zusammenhang aufgegeben, nach der Beendigung einer Verbindung unverzüglich die für die Berechnung des Entgelts erforderlichen Daten zu ermitteln. Nur diese Abrechnungsdaten dürfen bis zu sechs Monate nach Versendung der Rechnung gespeichert werden. Alle nicht erforderlichen Daten sind hingegen unverzüglich zu löschen. Diese Regelungen sind von der Entscheidung des BVerfG zur Vorratsdatenspeicherung[10] unberührt und weiterhin gültig. Dasselbe gilt für die Regelung zur Speicherung der Standortdaten. Hier war und ist § 98 TKG einschlägig.

### *2.1.3 Zugriff*

Der Zugriff auf die Verkehrsdaten ist zum einen im Bundesrecht für den repressiven Einsatzbereich in § 100g StPO geregelt. Bis zu dem Urteil des BVerfG zur Vorratsdatenspeicherung gewährte die Vorschrift den Zugriff auf Verkehrsdaten, die nach § 96 Abs. 1 oder nach § 113a TKG erhoben worden waren. Aufgrund des Wegfalls der letztgenannten Speicherpflicht verbleibt es bei den Zugriffsmöglichkeiten auf die oben näher dargelegten Datenbestände. Zum anderen kann der Zugriff auch von den Ländern für den präventiven Einsatzbe-

---

[9] Ausführlicher zu den unterschiedlichen Arten der Telekommunikationsüberwachung *Kilchling* 2011.

[10] BVerfG, 1 BvR 256/08 v. 2.3.2010, z.B. NJW 2010, S. 803, NStZ 2010, S. 341, NVwZ 2010, S. 770.

reich geregelt werden. Dies hat das BVerfG in seiner Entscheidung zur Vorratsdatenspeicherung explizit festgestellt.[11]

Der Zugriff selbst erfolgt durch eine Abfrage bei dem oder den jeweils zuständigen Telekommunikationsanbietern. Die Polizei kann insoweit nicht selbst tätig werden.

### *2.2 Ortung von Mobiltelefonen gem. § 33b Abs. 3 Nr. 2 BbgPolG*

Bei der Mobilfunkortung handelt es sich um eine Maßnahme, die die Verkehrsdatenabfrage gem. § 33b Abs. 6 S. 2 BbgPolG ergänzt. Sie wird – anders als die Maßnahmen gem. § 33b Abs. 6 S. 2 BbgPolG – von der Polizei selbst durchgeführt und dient zum einen der Identifizierung unbekannter Mobiltelefone. Diese kann notwendig werden, wenn die Polizei – etwa im Rahmen einer längerfristigen Observation – beobachtet, dass ein Verdächtiger eines oder mehrere Handys benutzt, die Beamten aber weder die Karten- noch die Gerätenummern kennen. In dieser Einsatzform kann die Maßnahme eine künftige Verkehrsdatenabfrage vorbereiten. Zum anderen kann die Maßnahme in bestimmten Situationen der exakten Lokalisierung von bereits bekannten Mobiltelefonen dienen. In dieser Funktion kann sie eine Verkehrsdatenabfrage ergänzen oder sogar ersetzen. Mögliche Beispiele sind die Suche nach einer vermissten oder suizidgefährdeten Person, die sich in einer sehr großflächigen Funkzelle (z.B. im Wald oder einem anderen schwach besiedelten Gebiet) aufhält und daher mit einer Standortdatenabfrage nur sehr grob lokalisiert werden kann, oder die Situation einer Geiselnahme in einem größeren Gebäude, in welchem der genaue Aufenthaltsort des oder der Täter durch Lokalisierung ihrer Mobiltelefone recht zielgenau möglich ist. Das technische Instrument zur Durchführung der Maßnahme ist der sog. IMSI-Catcher.

Um die Nutzung von Mobiltelefonen möglichst flächendeckend zu ermöglichen, sind die von den Mobilfunkunternehmen bereitgestellten Mobilfunknetze in Funkzellen unterteilt. In der Mitte dieser Funkzelle befindet sich ein Sendemast, die sog. Basisstation. Die Reichweite einer Funkzelle hängt von der Bevölkerungsdichte ab: während sie sich in dicht bevölkerten Gegenden nur über wenige hundert Meter erstreckt, kann eine Funkzelle im ländlichen Bereich mehrere Kilometer abdecken.[12]

Bei dem IMSI-Catcher handelt es sich um ein technisches Gerät, welches eine solche Funkzelle simuliert. Diese „virtuelle“[13] Funkzelle hat eine stärkere Leistung als die von den Telekommunikationsanbietern bereitgestellten Funkzellen. Dadurch wählen sich alle eingeschalteten Mobiltelefone, die sich im Empfangsbereich der simulierten Funkzelle befinden, automatisch in diese ein, anstatt auf die von den Telekommunikationsunternehmen bereitgestellten Funkzellen zuzugreifen. Dies gilt auch für Telefone, die lediglich eingeschaltet sind, momentan aber nicht genutzt werden (Stand-By-Betrieb). Der IMSI-Catcher liest die welt-

---

[11] BVerfG, 1 BvR 256/08 v. 2.3.2010, Leitsatz 5, Abs. 230 ff.

[12] *Harnisch/Pohlmann*: Strafprozessuale Maßnahmen bei Mobilfunkendgeräten – Die Befugnis zum Einsatz des sog. IMSI-Catchers, in: HRRS 2009, 202, 203.

[13] BVerfG MMR 2006, 805, 808.

weit nur einmal vergebene IMSI[14]- und IMEI[15]-Nummer aller eingewählten Mobiltelefone aus.[16] Bei der IMSI-Nummer handelt es sich um eine Kennnummer von SIM-Karten, die IMEI-Nummer wird hingegen dem Mobiltelefon zugeordnet (Gerätekennung).[17]

Diese Daten können nun zur gezielten Ortung eines bereits bekannten oder zur Identifizierung eines bislang unbekannten Mobiltelefons verwendet werden. Sofern ein bestimmtes Mobiltelefon, dessen Identifikationsdaten der Polizei bekannt sind, lokalisiert werden soll, wird mit dem IMSI-Catcher in derjenigen Funkzelle, in der das Mobiltelefon eingewählt ist oder zuletzt eingewählt war, eine Funkzelle geringerer Ausdehnung simuliert. Befindet sich das gesuchte Mobiltelefon in diesem Bereich, kann die simulierte Funkzelle weiter verkleinert und eine erneute Suche durchgeführt werden.[18] Dieser Vorgang kann so oft wiederholt werden, bis sich die Funkzelle auf wenige Meter beschränkt oder sich das Mobiltelefon sogar punktgenau lokalisieren lässt.

Soll hingegen ermittelt werden, welches Mobiltelefon einem Störer oder Straftäter zuzuordnen ist, muss der IMSI-Catcher an einem oder mehreren Orten, an denen die gesuchte Person vermutet wird, wiederholt eingesetzt werden. Wird eine IMSI- oder IMEI-Nummer dabei mehrfach von dem IMSI-Catcher ermittelt, kann diese Nummer mit Hilfe der beim Telekommunikationsanbieter gespeicherten Bestandsdaten einer konkreten Person zugeordnet und diese ggf. überprüft werden.[19]

Des Weiteren kann der IMSI-Catcher zur Observation einer bestimmten Person eingesetzt werden.[20]

### *2.3 Anlassbezogene automatische Kennzeichenfahndung*

#### *2.3.1 Terminologie*

Obwohl zur Kennzeichenfahndung in den verschiedenen Bundesländern im Wesentlichen dieselbe Technik eingesetzt wird, hat sich für die Maßnahme bislang noch keine einheitliche Terminologie herausgebildet. Dies kann teilweise mit den unterschiedlichen rechtlichen Rahmenbedingungen erklärt werden, die gerade bei neuen Maßnahmen ihre Bezeichnung beeinflussen. So wird die Maßnahme teilweise als „automatisierte (Kfz-) Kennzeichenerken-

---

[14] International Mobile Subscriber Identity.

[15] International Mobile Equipment Identity.

[16] Karlsruher Kommentar zur StPO-Nack, 6. Auflage, § 100i Rn. 5; *Harnisch/Pohlmann*: Strafprozessuale Maßnahmen bei Mobilfunkendgeräten – Die Befugnis zum Einsatz des sog. IMSI-Catchers, in: HRRS 2009, 202; *Roggan*: Moderne Telekommunikationsüberwachung: Eine kritische Bestandsaufnahme, in: KritV 2003, 76, 86.

[17] *Harnisch/Pohlmann*: Strafprozessuale Maßnahmen bei Mobilfunkendgeräten – Die Befugnis zum Einsatz des sog. IMSI-Catchers, in: HRRS 2009, 202 f.; Nachbaur: Standortfeststellung und Art. 10 GG – Der Kammerbeschluss des BVerfG zum Einsatz des „IMSI-Catchers", NJW 2007, 335.

[18] *Roggan*: Moderne Telekommunikationsüberwachung: Eine kritische Bestandsaufnahme, in: KritV 2003, 76, 86.

[19] Vgl. Karlsruher Kommentar zur StPO-Nack, 6. Auflage, § 100i Rn. 6.

[20] Karlsruher Kommentar zur StPO-Nack, 6. Auflage, § 100i Rn. 6.

nung“[21], „(automatisierte) Kennzeichenerfassung“[22] oder als Einsatz sog. „Kennzeichenerfassungssysteme“[23] bezeichnet. In der kritischen Literatur findet daneben häufiger der Begriff „Kfz-Massenabgleich“[24] Verwendung.

Das Polizeigesetz des Landes Brandenburg spricht in § 36a demgegenüber von der „anlassbezogenen automatischen Kennzeichenfahndung“. Damit verweist das Gesetz explizit auf den Zweck der Maßnahme, nämlich die Fahndung nach bestimmten konkreten Fahrzeugen. So wird deutlich, dass es sich nicht um eine anlasslose Überwachungs-, sondern um eine anlassbezogene, d.h. zielgerichtete Fahndungsmaßnahme handelt. Dies lässt den Begriff gegenüber den möglichen deutschen bzw. deutschsprachigen Alternativtermini unbedingt vorzugswürdig erscheinen.

Auch im Ausland hat sich für die automatische Kennzeichenfahndung bislang noch keine einheitliche Terminologie herauskristallisiert. So wird die Maßnahme in der englischsprachigen Literatur gleichermaßen als „Automatic Number Plate Recognition“ (ANPR), als „License Plate Recognition“ (LPR), als „Automatic Vehicle Identification“ (AVI), als „Car Plate Reader“ (CPR) und als „Optical Character Recognition for Cars“ (OCR) bezeichnet.[25] Dabei scheint sich die Bezeichnung ANPR nach und nach durchzusetzen.

### *2.3.2 Implementation und Durchführung*

#### 2.3.2.1 Fahndungsmodus

Die technische Durchführung der automatischen Kennzeichenfahndung erfolgt mit Hilfe einer Kamera, die wahlweise fest installiert sein kann, insbesondere an Brücken (stationäre Systeme), nur für den jeweiligen Einsatz aufgebaut (halbstationärer Einsatz) oder aus einem fahrenden Auto heraus eingesetzt werden kann (mobiler Einsatz).[26] Die Kamera arbeitet aus der Rückansicht und ist direkt mit einer EDV-Einheit verbunden, in welcher der elektronische Abgleich mit der sog. Fahndungsdatei durchgeführt wird. In dieser Fahndungsdatei werden die Kraftfahrzeugkennzeichen geführt, nach denen jeweils aktuell gesucht wird. Abbildung 1 zeigt eines der stationären Systeme im Autobahnbereich.

---

[21] *Lang*, JurPC Web-Dok. 93/2005, Abs. 81 ff.; *Schieder*, NVwZ 2004, 778; ähnlich auch *Robrecht*, NJ 2008, 9.

[22] *Erd*, KJ 2008, 118, 120, 129 ff.; *Roßnagel*, NJW 2008, 2547, 2548; *Welsing*, S. 140 ff.; ähnlich *Zöller*, NVwZ 2005, 1235, 1236. Siehe auch den Titel des Artikels von *Baumann, Ruedi* im Tagesanzeiger (Online), 06.09.201: Polizei filmt am Sihlquai rund um die Uhr Autonummern.

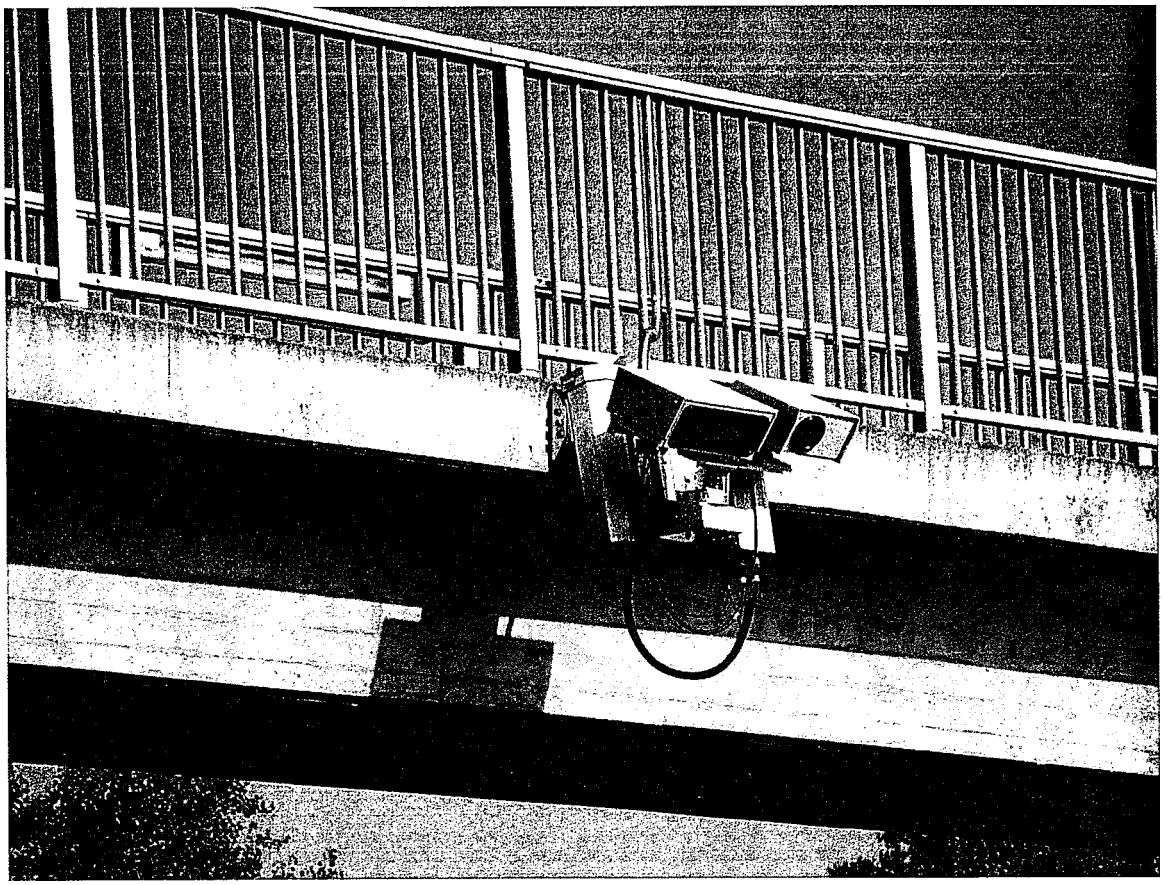
[23] *Robrecht*, NJ 2008, 9.

[24] *Breyer*, NVwZ 2008, 824.

[25] *Schieder*, NVwZ 2004, 778, Fn. 4.

[26] Siehe für nähere Einzelheiten z.B. *Schüler*, PVT 2007, 1; *Roßnagel*, NJW 2008, 2547.

*Abbildung 1: Stationäres Kamerasystem*



Nach Inbetriebnahme liest das System die Kennzeichen aller passierenden Fahrzeuge aus und wandelt diese in eine konsekutive Buchstaben-Zahlen-Kombination um. Das fiktive Kennzeichen AB – C 1234 würde also in ABC1234 umgewandelt werden. Entsprechendes gilt für das brandenburgische Polizeifahrzeug mit dem Kennzeichen BBL 4 – 4200 (siehe Abb. 2a), das zu Testzwecken eingesetzt wurde; dieses wird von dem System als BBL44200 eingelesen. Diese abstrakte Buchstaben-Zahlen-Kombination wird automatisch mittels Einsatz einer entsprechenden Software mit dem Inhalt der Fahndungsdatei abgeglichen.[27] Ergibt der Abgleich keine Übereinstimmung des erfassten Kennzeichens mit der Fahndungsdatei, werden sämtliche über dieses Fahrzeug erhobenen Daten in der Regel unverzüglich, selbständig und spurlos gelöscht. Diese Löschung kann nicht verhindert oder rückgängig gemacht werden.

---

[27] *Zöller*, NVwZ 2005, 1235; *Schieder*, NVwZ 2004, 778.

*Abbildung 2a: Trefferbild 1*


Liegt hingegen ein Trefferfall vor, ergeht bei der zuständigen Polizeidienststelle ein entsprechendes Signal. Auf dem Bildschirm des zuständigen Beamten – nur einzelne, speziell dazu ermächtigte Personen haben Zugang zu dem System – erscheinen das ausgelesene Kennzeichen samt Foto sowie der dazugehörige Eintrag aus der Fahndungsliste. Dies ermöglicht der Polizei einen manuellen Abgleich der Identität des erfassten Kennzeichens mit dem gesuchten Kennzeichen, bevor weitere Maßnahmen eingeleitet werden. Auf diese Weise wird die konkrete Zuordnung überprüft und verhindert, dass aufgrund einer möglicherweise fehlerhaften Rück-Umwandlung des Kennzeichens auf der Grundlage der abstrakten Buchstaben-Zahlen-Kombination polizeiliche Maßnahmen gegen ein falsches Fahrzeug eingeleitet werden. Denn die für das o.g. Suchkennzeichen AB – C 1234 gespeicherte Buchstaben-Zahlen-Kombination –AAB1234 – würde nicht nur für das Fahndungsobjekt selbst eine Treffermeldung auslösen, sondern auch bei anderen Kennzeichen, die mit identischer abstrakter Buchstaben-Zahlen-Abfolge eingelesen würden wie beispielsweise das Kennzeichen A – BC 1234. Der manuelle Abgleich dient dazu, eine derartige Treffermeldung als Fehltreffer zu erkennen. Sämtliche Daten über das fälschlicherweise erfasste Kraftfahrzeug werden in diesem Fall manuell gelöscht.

Nur wenn tatsächlich ein echter Trefferfall vorliegt, veranlasst der zuständige Polizeibeamte die notwendigen Anschlussmaßnahmen.

Die Systeme, die in Brandenburg zur automatischen Kennzeichenfahndung eingesetzt werden, können etwa 7.000 Fahrzeuge pro Stunde erfassen und mit dem Fahndungsbestand abgleichen[28]; ein einzelner Vorgang dauert nur Sekundenbruchteile. Die Geräte sind auch in der Lage, ausländische Kennzeichen zu erkennen und entsprechend auszulesen.[29] Aufgrund der eingesetzten Infrarot-Technik liefern die Geräte auch bei schlechtem Wetter und verschmutzten Kennzeichen zuverlässige Ergebnisse.[30]

Neben den gesuchten Kennzeichen enthält die Fahndungsdatei zu jedem Eintrag noch das Eingabedatum, eine interne Identifikationsnummer sowie einen kurzen Vermerk zu dem jeweiligen Sachverhalt. Dort kann beispielsweise notiert werden, weshalb nach dem Kfz gefahndet wird oder ob der gesuchte Fahrer möglicherweise bewaffnet ist. Ferner muss die Suche zeitlich befristet werden. Der eingegebene Datensatz wird dann nach dem Zeitablauf

---

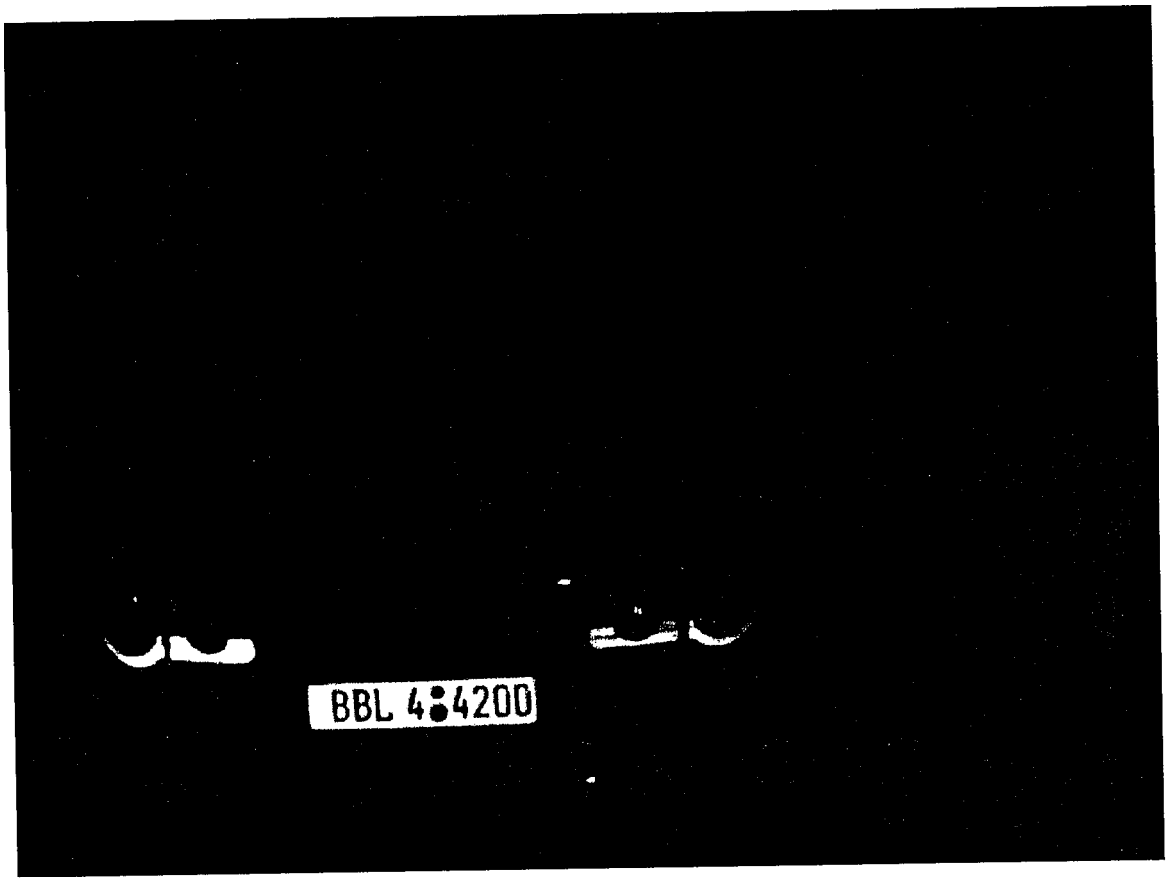
[28] In der Literatur wird teilweise eine geringere Kapazität angegeben; so gehen z.B. *Roßnagel*, NJW 2008, 2547 oder *Arzt*, SVR 2004, 321 von 3.000 auslesbaren Kennzeichen pro Stunde aus.

[29] *Arzt*, SVR 2004,321.

[30] *Zöller*, NVwZ 2005, 1235 f.

automatisch aus der Fahndungsdatei herausgenommen. Das System ist in Brandenburg so konfiguriert, dass eine Fahndung ohne Eingabe eines Löschdatums nicht aktiviert werden kann.

*Abbildung 2b: Trefferbild 2*




Liegt ein Trefferfall vor, werden neben dem ausgelesenen Kennzeichen (siehe Abb. 2a) und einem Foto des betroffenen Fahrzeugs (ebenfalls in Rückansicht, siehe Abb. 2b) noch Datum, Uhrzeit und Ort der Aufnahme sowie gegebenenfalls die Fahrtrichtung gespeichert.[31] Das Foto zeigt lediglich Konturen, Insassen sind in der Regel nicht zu erkennen und wären wegen der Rückansicht ohnehin nicht identifizierbar.

2.3.2.2 Aufzeichnungsmodus

In Brandenburg und einigen anderen Bundesländern wird die zur automatischen Kennzeichenfahndung verfügbare Technik neben dem Einsatz zu Fahndungszwecken auch in einem Aufzeichnungsmodus betrieben. Dabei werden ebenfalls die Kennzeichen aller die Kontrolleinrichtung passierenden Fahrzeuge erfasst und eingelesen. Sie werden aber nicht mit einem konkreten Fahndungsbestand abgeglichen. Zweck der Maßnahme ist vielmehr die längerfris-

---

[31] In Brandenburg wird die Fahrtrichtung dabei lediglich bei mobilen Einsätzen direkt miterfasst. Bei den stationären Systemen ergibt sich die Fahrrichtung generell aus dem festen Standort.

tige Speicherung der erfassten Fahrzeugdaten, um sie je nach Bedarf ermittlerisch weiterverarbeiten zu können.

Diese Maßnahme ist ausschließlich repressiver Natur und wird regelmäßig im Zusammenhang mit Observationen durchgeführt. Rechtsgrundlage sind die §§ 100h, 111, 163e, 163f StPO. Die einschlägigen Fälle fließen vorliegend mit in die statistische Grundauswertung ein, um ein realistisches Abbild des Einsatzes der automatischen Kennzeichenfahndung in Brandenburg präsentieren und den Anteil zwischen den repressiven und präventiven Einsatzvarianten wirklichkeitsnah darstellen zu können. Eine rechtliche Bewertung dieser Einsatzform würde den Untersuchungsauftrag allerdings überdehnen.

#### 2.3.2.3 Zählung von Kraftfahrzeugen

Schließlich kann die zur automatischen Kennzeichenfahndung dienende Technik auch zur rein quantitativen Zählung aller oder bestimmter eine konkrete Stelle passierenden Fahrzeuge eingesetzt werden. Auswahlparameter können insbesondere bestimmte Kennzeichenfragmente sein, etwa ein bestimmter Stadt- oder Landkreis. Bei Durchführung einer solchen Fahrzeugzählung werden keine individuellen Kennzeichen erfasst, mit einem Fahndungsbestand abgeglichen oder gespeichert; vielmehr werden alle Fahrzeuge, die das jeweilige Suchkriterium erfüllen – beispielsweise alle im Vorfeld eines Spieltages der Fußball-Bundesliga aus Richtung Rostock nach Cottbus einfahrenden Fahrzeuge mit dem Kennzeichenfragment HRO – lediglich gezählt.

Die zuständigen Ordnungsbehörden setzen diese Form der Fahrzeugzählung insbesondere vor Fußballspielen, Großkonzerten oder Rockertreffen ein, um abschätzen zu können, wie viele Personen die Veranstaltung voraussichtlich besuchen werden und wie viele Polizeikräfte bereitgestellt werden müssen.

### *2.3.3 Abgrenzung der automatischen Kennzeichenfahndung von anderen Maßnahmen*

Während automatische Kennzeichenlesesysteme im privaten Bereich schon seit geraumer Zeit beispielsweise zur Überprüfung von Zufahrtsberechtigungen eingesetzt werden,[32] stellt die automatische Kennzeichenfahndung im Instrumentarium der Polizei immer noch eine relativ neue Maßnahme dar. Sie ergänzt die bisherigen Polizeimaßnahmen zur Kontrolle einer Vielzahl von Personen und muss daher von bereits länger praktizierten Maßnahmen, die eine vergleichbare Breitenwirkung besitzen, abgegrenzt werden.

#### 2.3.3.1 Rasterfahndung

Bei Durchführung einer Rasterfahndung[33] sucht die Polizei zunächst nach Merkmalen, die ihren Erkenntnissen zufolge auf die gesuchte Person zutreffen, und erstellt anhand der gewonnenen Informationen ein Täterprofil, das sog. Raster.[34] Anschließend sammelt sie Daten, die für die konkrete Maßnahme relevant erscheinen, indem sie diese selbst erhebt oder von

---

32 *Schieder*, NVwZ 2004, 778.

33 Hierzu ausführl. *Pehl* 2008.

34 *Gusy*, KritV 2002, 474, 483f.; *Schenke*, § 3 Rn. 213.

öffentlichen und privaten Stellen – ggf. zwangsweise[35] – einholt.[36] Die gesammelten Daten werden schließlich automatisch unter Nutzung einer speziellen Software mit den eigenen Datenbeständen der Polizei abgeglichen und nach den festgelegten Kriterien durchsucht (sog. Rasterung).[37] Sofern die überprüften Daten eine Übereinstimmung mit dem Täterprofil aufweisen, bleiben sie in dem Raster hängen. Alle anderen Daten werden ausgesondert und gelöscht.[38]

Die Rasterfahndung ist also eine Form der vernetzten Durchsuchung von *außerpolizeilichen Datenbeständen*. Ihr Ziel ist es, die Gruppe der zu überprüfenden Personen einzugrenzen, indem all diejenigen Personen ausgefiltert werden, die als Täter oder Störer eindeutig nicht in Betracht kommen.[39] Wer im Raster hängen bleibt, weist bestimmte, für die weiteren Ermittlungen bedeutsame Merkmale auf.[40] Da der Abgleich auf elektronischem Wege erfolgt, werden auch nur die Daten dieser Betroffenen menschlich wahrgenommen.[41] Insofern erscheint die Situation derjenigen bei der automatischen Kennzeichenfahndung vergleichbar. Je dichter das Fahndungsnetz geknüpft ist, desto höher ist dessen Spezifität, mit der Konsequenz, dass dann weniger Personen, sei es als Tatverdächtige oder potentielle Störer, weiteren polizeilichen Maßnahmen unterzogen werden. Diese sind dann jedoch nicht mehr Bestandteil der Rasterfahndung als solcher, sondern stellen Anschlussmaßnahmen dar, die einer eigenen Ermächtigungsgrundlage bedürfen.[42]

Die Rasterfahndung wurde in den 1970er Jahren zunächst ohne spezielle Ermächtigungsgrundlage zur Fahndung nach steckbrieflich gesuchten mutmaßlichen RAF-Terroristen eingesetzt.[43] Erst Anfang der 1990er Jahre wurde sie im Kampf gegen die organisierte Kriminalität wiederentdeckt und 1992 durch das Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität (OrgKG)[44] in §§ 98a, 98b StPO auf eine gesetzliche Grundlage gestellt.[45] Inzwischen hat sie auch Eingang in die Polizei- und Ordnungsgesetze aller Bundesländer gefunden[46] und wird nunmehr sowohl zu präventiven Zwecken als auch zur Strafverfolgung eingesetzt.[47]

Rasterfahndung und automatische Kennzeichenfahndung verfolgen also – obwohl sie gleichermaßen eine Vielzahl von Personen erfassen und deren Daten mit einem Datenbestand

---

35 Vgl. §§ 98a V, 95 II StPO; *Riegel*, ZRP 1980, 300; *Roxin/Schünemann*, § 32 Rn. 13.

36 *Volkmann*, Jura 2007, 132, 133; *Riegel*, ZRP 1980, 300; *Götz*, § 17 Rn. 61.

37 BVerfGE 115, 320, 321; *Volkmann*, Jura 2007, 132, 133; *Riegel*, ZRP 1980, 300.

38 *Volkmann*, Jura 2007, 132, 133; Vgl. auch *Horst Herold* in einem Spiegel-Interview, Der Spiegel, Nr. 37/1986, S. 52.

39 *Riegel*, ZRP 1980, 300, 301.

40 BVerfGE 115, 320, 321.

41 *Riegel*, ZRP 1980, 300, 301.

42 *Volkmann*, Jura 2007, 132, 133.

43 BVerfGE 115, 320, 321; *Volkmann*, Jura 2007, 132, 133; *Gusy*, KritV 2002, 474.

44 BGBl. I S. 1302.

45 *Götz*, § 18 Rn. 7.

46 Siehe § 46 BbgPolG.

47 *Volkmann*, Jura 2007, 132, 133.

abgleichen – unterschiedliche Zwecke: Während die automatische Kennzeichenfahndung zur gezielten Suche nach bekannten Tatverdächtigen oder Störern eingesetzt wird, dient die Rasterfahndung der Eingrenzung des Personenkreises von Tatverdächtigen oder potentiellen Störern und damit der Ermittlung einer bislang unbekannten Zielperson. Sie setzt also nicht an einem bereits bestehenden Verdacht gegen eine konkrete Person an, sondern dient vielmehr zur Gewinnung eines solchen Verdachts.

#### 2.3.3.2 Schleierfahndung

Bei der Schleierfahndung handelt es sich, im Gegensatz zu der automatischen Kennzeichen- und der Rasterfahndung, um eine konventionelle, nicht-automatisierte Fahndungsmethode. Der Begriff bezieht sich auf schlichte „Jedermannkontrollen“[48], die insbesondere der vorbeugenden Bekämpfung grenzüberschreitender Kriminalität dienen sollen.[49] Als rein präventivpolizeiliche Maßnahme[50] ist die Schleierfahndung ausschließlich in den Polizei- und Ordnungsgesetzen der Länder[51] und des Bundes[52] geregelt. Sie darf in Grenzgebieten, in bestimmten Bereichen des öffentlichen Straßenverkehrs sowie in bestimmten Einrichtungen des öffentlichen Verkehrs nach pflichtgemäßem Ermessen der Polizei durchgeführt werden, ohne dass ein konkreter Verdacht oder ein konkreter Anlass vorliegen muss.[53]

Die Maßnahme soll den Wegfall der Personenkontrollen an den nationalen Außengrenzen zu den Schengen-Vertragsstaaten kompensieren[54] und wird vor allem in einem 30-km-Streifen entlang der Bundesgrenzen – dem sog. „Sicherheitsschleier“[55] –, auf Durchgangsstraßen sowie in Zügen, auf Bahnhöfen und an Flughäfen durchgeführt.[56] Auch wenn die Schleierfahndung teilweise als nicht intendierte „Verlagerung der früheren Grenzkontrollmöglichkeiten ins Landesinnere“[57] kritisiert wird, ist sie mit dem Schengener Durchführungsübereinkommen (SDÜ) vereinbar.[58]

#### 2.3.3.3 Schleppnetzfahndung

Erlangt die Polizei anlässlich einer grenzpolizeilichen Kontrolle oder an einer Kontrollstelle i.S.d. § 111 StPO Daten, die bestimmte Suchkriterien aufweisen und zur Erfüllung ihrer strafprozessualen Aufgaben von Bedeutung sein könnten, dürfen diese im Rahmen einer

---

48 *Lisken*, NVwZ 1998, 22.

49 *Götz*, § 17 Rn. 29.

50 *Roxin/Schünemann*, § 32 Rn. 11.

51 Siehe §§ 11 III, 12 I Nr. 6 BbgPolG, siehe zum Ganzen: *Graf*, S., S. 45 ff.

52 Siehe §§ 22 I a, 23 I Nr. 3 BPolG.

53 *Götz*, § 17 Rn. 30; *Graf, S.*, S. 24; *Schenke*, § 3 Rn. 120.

54 *Lisken*, NVwZ 1998, 22 f.

55 Innenminister *Manfred Kanther*, Dezember 1995. Aus diesem Begriff rührt auch die Bezeichnung „Schleierfahndung“ her, vgl. *Graf, S.*, S. 24; *Götz*, § 17 Rn. 28; *Lisken*, NVwZ 1998, 23.

56 *Götz*, § 17 Rn. 28, 31; *Ruder/Schmitt*, Rn. 558b; *Schenke*, § 3 Rn. 120.

57 *Lisken*, NVwZ 1998, 23.

58 Siehe Art. 2 III SDÜ. *Graf*, S., S. 342 ff., insbes. S. 345.

Schleppnetzfahndung gem. § 163d StPO gespeichert und nach § 483 StPO ausgewertet werden.[59] Die von der Maßnahme betroffene Person muss dabei nicht selbst einer Straftat verdächtig sein; entscheidend ist lediglich, dass die erlangten Daten den vorher festgelegten Kriterien entsprechen.[60] Die Schleppnetzfahndung ermöglicht also die Speicherung und den Abgleich von Daten, die regelmäßig – insbesondere bei Massenkontrollen – sofort nach ihrer Erhebung wieder verloren gehen.[61]

Zu beachten ist, dass es sich bei den festgelegten Kriterien nicht um ein vorgegebenes Raster handelt, in dem der Verdächtige „hängen bleiben" soll. Vielmehr sollen mit Hilfe der Schleppnetzfahndung diejenigen Informationen gesammelt werden, die zur Erstellung eines solchen Rasters notwendig wären. Die Maßnahme ermöglicht es also, „die Maschen vieler polizeilicher Personenkontrollen" zu einem „täterundurchlässigen Netz" zu verknüpfen.[62]

Sowohl bei der automatischen Kennzeichenfahndung als auch bei der Schleppnetzfahndung soll der Verdächtige mit Hilfe eines automatischen Datenabgleichs „aus dem Kreis der Unverdächtigen filtriert werden"[63]. Die beiden Maßnahmen unterscheiden sich jedoch darin, dass die Zielperson des Verfahrens im Fall einer automatischen Kennzeichenfahndung bereits bekannt ist, die Schleppnetzfahndung hingegen erst zu dem noch unbekannten Tatverdächtigen führen soll.

Von der rein präventiven Schleierfahndung lässt sich die Schleppnetzfahndung durch ihre ausschließlich repressive Zwecksetzung abgrenzen.[64]

#### 2.3.3.4 Kontrollstelle

Eine Kontrollstelle ist eine von der Polizei errichtete Sperrung, an der Personen zwecks Überprüfung und Identitätsfeststellung angehalten werden. Ihre Errichtung ist sowohl nach den Polizeigesetzen des Bundes[65] und der Länder[66] als auch nach § 111 StPO nur zur Verhütung bzw. Verfolgung bestimmter – wenn auch je nach Vorschrift unterschiedlicher – Katalogstraftaten zulässig. Jeder, der eine solche Kontrollstelle passiert, ist dazu verpflichtet, seine Identität feststellen und die von ihm mitgeführten Sachen durchsuchen zu lassen. § 111 StPO ermöglicht also eine generelle Kontrolle aller Personen, die eine bestimmte Stelle passieren.[67] Aus der Verweisung des § 111 Abs. 3 StPO auf § 163b StPO und der darin enthaltenen Weiterverweisung auf die §§ 69 Abs. 1, 163a Abs. 4 StPO bzw. aus der Verweisung des § 111 StPO auf § 106 StPO ergibt sich, dass jeder, der angehalten und kontrolliert wird, auf den Grund dieser Maßnahmen hingewiesen werden muss.[68] Über die Identitätsfeststellung

---

59 *Schoreit*, DRiZ 1987, 82; *Roxin/Schünemann*, § 32 Rn. 10.

60 *Beulke*, Rn. 261.

61 *Roxin/Schünemann*, § 32 Rn. 10.

62 Vgl. *Horst Herold* in einem Spiegel-Interview, Der Spiegel, Nr. 37/1986, S. 49.

63 *Beulke*, Rn. 261.

64 *Roxin/Schünemann*, § 32 Rn. 10.

65 § 23 II Nr. 3, 44 III Nr. 3 BPolG.

66 Siehe § 22 I Nr. 6, II BbgPolG.

67 *Beulke*, Rn. 260.

68 Löwe/Rosenberg-*Schäfer*, § 111 Rn. 26; *Meyer-Goßner*, § 111 Rn. 10.

und Durchsuchung hinausgehende Anschlussmaßnahmen bedürfen jedoch einer speziellen Ermächtigungsgrundlage.[69] In der Bundesrepublik ist die Maßnahme insbesondere im Vorfeld von Großdemonstrationen von Bedeutung.

In ihrer repressiven Variante spricht man auch von Ringalarmfahndung. Sie kann mit der automatischen Kennzeichenfahndung kombiniert werden, insbes. wenn Verdächtige in einem Kfz auf der Flucht sind, dessen Kennzeichen oder möglicherweise auch nur – etwa von Zeugen bei einem Banküberfall erkannte – Kennzeichenfragmente bekannt sind. Aus ermittlungstaktischen Gründen kann die Kennzeichenfahndung bei der Ringalarmfahndung auch im Aufzeichnungsmodus betrieben werden, um die Aufzeichnungen bei der Ermittlungsarbeit auswerten zu können. Diese Einsatzvariante kommt der traditionellen Form der früher in solchen Fällen mitunter eingesetzten manuellen Aufzeichnung der Kennzeichen vorbeifahrender Kfz durch speziell postierte Polizeibeamte sehr nahe, ist aber wesentlich effektiver und schont zugleich die knappen Personalressourcen der Polizei.

### *2.4 Exkurs: An der Schnittstelle zwischen präventivem und repressivem Einsatz: Die Doppelfunktionalität polizeilichen Handelns*

Sowohl die automatische Kennzeichenfahndung als auch die Verkehrsdatenabfrage und die Mobilfunkortung sind technische Instrumente, die sowohl präventiv zur Gefahrenabwehr als auch repressiv, also zur Strafverfolgung, eingesetzt werden können. Dies ergibt sich aus der Doppelfunktion der Polizei als zuständige Behörde zur Gefahrenabwehr und als repressiv tätiges Ermittlungsorgan. Dieser Aufgabendualismus[70] der Polizei führt dazu, dass die Maßnahmen je nach Einsatzbereich auf unterschiedliche Ermächtigungsgrundlagen – StPO oder die jeweils einschlägigen Polizeigesetze – gestützt werden müssen. Denkbar ist ferner, dass die Maßnahme zugleich präventive und repressive Zwecke verfolgt. Dies stellt in der polizeilichen Praxis keine Besonderheit, sondern ein alltägliches Phänomen dar.[71] Ein besonders einleuchtendes Beispiel ist der Diebstahl von Kraftfahrzeugen (sog. Totalentwendung), der in Brandenburg einen bedeutsamen Anteil der Einsatzfälle der automatischen Kennzeichenfahndung ausmacht.

Die Zuordnung einer doppelfunktionalen Maßnahme zum präventiven oder repressiven Bereich entscheidet insbesondere darüber, ob die Polizei bzw. die Staatsanwaltschaft entsprechend dem in §§ 152 Abs. 2, 163 Abs. 1 StPO verankerten Legalitätsprinzip zum Einschreiten verpflichtet ist oder ob die Polizei auf der Grundlage des Opportunitätsprinzips nach eigenem Ermessen tätig werden kann. Die jeweils einschlägige Ermächtigungsgrundlage bestimmt dann, welchen Voraussetzungen die Maßnahme unterliegt, insbesondere ob bei Beginn der Maßnahme ein Anfangsverdacht oder eine konkrete Gefahr gegeben sein muss und wer die Maßnahme anordnen darf. Zudem entscheidet die Zuordnung darüber, ob die Staatsanwaltschaft bei Durchführung der Maßnahme gegenüber der Polizei weisungsbefugt ist, bei wem die Einsatzleitung liegt und ob das Justiz- oder Innenressort zur Rechtsaufsicht berufen ist.

---

69 *Götz*, § 17 Rn. 26.

70 *Nolte*, Kriminalistik 2007, 343.

71 *Kniesel*, ZRP 1987, 377, 378.

Wird einer hoheitlichen Anordnung nicht Folge geleistet, richtet sich ihre zwangsweise Durchsetzung bei doppelfunktionalen Maßnahmen ebenfalls nach dem Rechtsgebiet, welchem die Maßnahme selbst zugeordnet wird. Des Weiteren legt die Zuordnung fest, wer die angefallenen Kosten zu tragen hat, wann über Sekundäransprüche entschieden wird und welchem Ressort die zu erstattenden Gelder zufließen. Auch ob und nach welchen Regeln die erlangten Daten weiterverwendet werden dürfen, hängt bei doppelfunktionalen Maßnahmen von deren Zuordnung zum präventiven oder repressiven Bereich ab.

Sofern der Betroffene gegen eine doppelfunktionale Maßnahme Rechtsmittel ergreifen möchte, muss er wissen, ob er zunächst Widerspruch einlegen und welchen Rechtsweg er gegebenenfalls einschlagen muss. Aus diesen gleichermaßen praktischen wie rechtstheoretischen Gründen[72] ist es unabdingbar, dass doppelfunktionale Maßnahmen eindeutig dem Gefahrenabwehrrecht oder der Strafverfolgung zugeordnet werden.[73]

---

72 Vgl. *Ehrenberg/Frohne*, Kriminalistik 2003, 737; *Emmerich*, DVBl. 1958, 338, 342.

73 *Zöller*, NVwZ 2005, 1235, 1240; *Roggan*, KritV 1998, 336 f.; *Achenbach*, JA 1981, 660, 662.

# Teil B: Nationaler Rechtsvergleich

## 1. Einleitung

Auch wenn sich die durchzuführende Evaluation nur auf die brandenburgischen Regelungen zur Verkehrsdatenabfrage, der Handyortung und der automatischen Kennzeichenfahndung bezieht, stellt der Vergleich mit der Rechtslage in den anderen Bundesländern eine wichtige Grundlage zur – späteren – Bewertung der brandenburgischen Regelungen dar. Mangels abweichender Regelung im Grundgesetz liegt die Gesetzgebungskompetenz für den Bereich der Gefahrenabwehr gem. Art. 70 Abs. 1 GG bekanntlich bei den Ländern.[74] Das bedeutet, dass jedes Bundesland diesen Bereich selbständig regelt, das Polizei- und Ordnungsrecht also von Land zu Land variiert. Im Folgenden werden diese Regelungen in einem deskriptiv gehaltenen Rechtsvergleich gegenübergestellt.

Bei diesem Vergleich ist zu beachten, dass es sich bei den hier zu überprüfenden Instrumenten noch immer um relativ neuartige polizeiliche Maßnahmen handelt. Auch wenn inzwischen viele Bundesländer entsprechende Ermächtigungsgrundlagen erlassen haben, ist der Gesetzgebungsprozess in diesem Bereich noch im Fluss. Das hängt auch mit dem Umstand zusammen, dass die Rechtsprechung in diesem Bereich – ungeachtet einiger Grundsatzentscheidungen durch das Bundesverfassungsgericht[75] – ebenfalls noch nicht gefestigt erscheint. Vielmehr ist damit zu rechnen, dass die aktuell bestehenden Regelungen geändert oder aufgehoben oder ganz neue Regelungen geschaffen werden könnten. Dies gilt insbesondere für die Länder Baden-Württemberg, Brandenburg, Hessen und Mecklenburg-Vorpommern, die die Rechtsgrundlagen für die fraglichen Maßnahmen jeweils mit einer Befristung versehen haben.[76] Teilweise besteht konkreter Anpassungsbedarf auch aufgrund der erwähnten verfassungsgerichtlichen Vorgaben.

Im Übrigen sind die Maßnahmen separat zu untersuchen, da sie jeweils auf unterschiedlichen Rechtsgrundlagen basieren, unterschiedliche Ziele verfolgen und, bedingt durch ihre technische Konfiguration, auch unter unterschiedlichen Rahmenbedingungen zum Einsatz kommen.

---

[74] Siehe v.a. *Wolf/Stephan/Deger*: Polizeigesetz für Baden-Württemberg, 6. Auflage (2009), § 23a Rn. 3; *Vollmar*: Telefonüberwachung im Polizeirecht (2008), S. 53ff.

[75] Siehe dazu im Einzelnen unten.

[76] In Baden-Württemberg: Verkehrsdatenabfrage und Standortermittlung befristet bis zum 31.12.2012, s. Art. 4 Abs. 2 i.V.m. Art. 1 Nr. 8 Gesetz zur Änderung des Polizeigesetzes, GBl. 2008, S. 390 (394, 401); in Brandenburg: Standortermittlung und automatische Kennzeichenfahndung befristet bis zum 31.12.2011, s. Art. 2 des Sechsten Gesetzes zur Änderung des Brandenburgischen Polizeigesetztes, GVBl. I 2008, S. 355; in Hessen: gesamtes HSOG befristet bis zum 31.12.2014, s. § 115 Abs. 2HSOG; in Mecklenburg-Vorpommern: alle drei Maßnahmen befristet bis zum 28.07.2011, s. § 116 SOG M-V.

## 2. Verkehrsdatenabfrage

Die Verkehrsdatenabfrage zu präventiven Zwecken ist in § 113b Nr. 2 TKG ausdrücklich vorgesehen und wird bislang in elf der sechzehn Bundesländer explizit geregelt. Welche Daten von dieser Maßnahme erfasst werden, ergibt sich aus §§ 3 Nr. 30, 96 Abs. 1 und 113a TKG. Danach sind Verkehrsdaten all diejenigen Daten, „die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden" (§ 3 Nr. 30 TKG), wie z.B. die Nummer oder Kennung der beteiligten Anschlüsse, Datum, Uhrzeit und Dauer der hergestellten Verbindungen sowie bei Mobiltelefonen die genutzte Funkzelle (vgl. §§ 96 Abs. 1, 113a TKG). Gesprächsinhalte werden von der Verkehrsdatenabfrage nicht erfasst.

Sofern die Bundesländer spezielle Regelungen zur präventiven Verkehrsdatenabfrage getroffen haben, sind zahlreiche Parallelen erkennbar. Besonders hervorzuheben ist, dass die Maßnahme in allen Bundesländern außer in Brandenburg und Mecklenburg-Vorpommern grundsätzlich einem Richtervorbehalt unterliegt.

### *2.1 Brandenburg*

**Auch wenn eine abschließende Analyse und Bewertung der brandenburgischen Regelung zur Verkehrsdatenabfrage im Rahmen der gegenwärtigen Evaluation noch aussteht, können in diesem Stadium bereits Struktur und Inhalt der Regelung in den Vergleich eingestellt werden.**

**Gemäß § 33b Abs. 6 S. 2 i.V.m. Abs. 1 i.V.m. § 33a Abs. 1 BbgPolG kann die Polizei von den Telekommunikationsunternehmen die unverzügliche Auskunft über Verkehrsdaten verlangen, sofern dies zur Abwehr einer dringenden Gefahr für Leib, Leben oder Freiheit einer Person unerlässlich ist oder aufgrund tatsächlicher Anhaltspunkte davon auszugehen ist, dass eine der in § 33a Abs. 1 Nr. 2 BbgPolG numerisch aufgezählten Straftaten organisiert begangen werden soll. In letzterem Fall wird ferner vorausgesetzt, dass die drohende Rechtsgutsverletzung auch im konkreten Einzelfall schwer wiegt und die Verkehrsdatenabfrage zur Abwehr der durch diese Straftaten drohenden Gefahr erforderlich ist.**

**Gem. § 33b Abs. 6 S. 2 i.V.m. Abs. 2 S. 2 BbgPolG darf sich die Maßnahme nur gegen den potentiellen Straftäter und dessen Kontakt- oder Begleitpersonen richten. Letztere sind in § 33a Abs. 2 S. 3 - 5 genau definiert.**

**Als einziges Bundesland hat das Land Brandenburg die Verkehrsdatenabfrage in keinem Fall einem Richtervorbehalt unterstellt. Die Anordnungsbefugnis richtet sich damit nach der allgemeinen Zuständigkeitsverteilung im brandenburgischen Polizeirecht.**

### *2.2 Baden-Württemberg*

In Baden-Württemberg ist die Verkehrsdatenabfrage in § 23a Abs. 5 Polizeigesetz Ba.-Wü. (PolG-BW) geregelt. Die Voraussetzungen werden in § 23a Abs. 5 i.V.m. Abs. 1 PolG-BW sehr genau beschrieben. Dabei wird unterschieden zwischen Handlungs- und Zustandsstörer i.S.d. §§ 6, 7 PolG-BW, Personen, die nach Erkenntnissen der Polizei die Begehung einer

Straftat planen, deren Gehilfen und Mitwisser, Personen, deren Telefoneinrichtungen von an der Planung Beteiligten verwendet werden, sowie unbeteiligten Personen i.S.d. § 9 PolG-BW. Die Verkehrsdaten von Handlungs- und Zustandsstörern i.S.d. §§ 6, 7 PolG-BW sowie von unbeteiligten Personen i.S.d. § 9 PolG-BW dürfen nur erhoben werden, soweit dies zur Abwehr einer unmittelbar bevorstehenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leben, Gesundheit oder Freiheit einer Peron erforderlich ist. Richtet sich die Maßnahme gegen eine andere in § 23a Abs. 1 Nr. 2 PolG-BW genannte Person, muss sie zur vorbeugenden Bekämpfung von schwerwiegenden Straftaten erforderlich sein. Welche Straftaten schwerwiegende im Sinne dieser Vorschrift sind, wird in § 23a Abs. 2 PolG-BW numerisch aufgelistet. Ergänzend wird gefordert, dass die aufgeführten Straftaten auch im konkreten Einzelfall schwer wiegen und tatsächliche Anhaltspunkte dafür vorliegen, dass sie dem Bereich der terroristischen, der organisierten oder der Bandenkriminalität zuzurechnen sind. Des Weiteren konkretisiert § 23a Abs. 1 S. 3 PolG-BW den Verhältnismäßigkeitsgrundsatz dahingehend, dass eine Verkehrsdatenabfrage nur erfolgen darf, „wenn sonst die Erfüllung der polizeilichen Aufgabe gefährdet oder wesentlich erschwert würde". Andererseits darf die Maßnahme gem. § 23a Abs. 1 S. 4 PolG-BW auch dann durchgeführt werden, wenn Dritte davon unvermeidbar betroffen sind.

Aus § 23a Abs. 5 i.V.m. Abs. 3 PolG-BW ergibt sich, dass die Verkehrsdatenabfrage in Baden-Württemberg, wie in den meisten anderen Bundesländern, einer richterlichen Anordnung bedarf. Diese kann nur ein kleiner Kreis von Führungspersonen beantragen: ein Regierungspräsident, der Leiter des LKA, der Leiter eines Polizeipräsidiums oder jener einer Polizeidienststelle. Allerdings sieht § 23a Abs. 3 S. 4 PolG-BW die Möglichkeit vor, dass diese Führungspersonen ihre Antragsbefugnis „auf besonders beauftragte Beamte des höheren Dienstes übertragen". Bei Gefahr im Verzug können gem. § 23a Abs. 3 S. 7 i.V.m. § 23 Abs. 3 S. 8 i.V.m. § 22 Abs. 6 PolG-BW die o.g. Führungspersonen, mit Ausnahme der Polizeidienststellenleiter, sowie der Leiter einer Polizeidirektion die Maßnahme anordnen.

§ 23a Abs. 3 S. 7 i.V.m. § 23 Abs. 3 S. 4, 5 PolG-BW sieht eine zeitliche Befristung der Verkehrsdatenabfrage auf drei Monate vor. Die Maßnahme kann jedoch um jeweils einen Monat verlängert werden, solange die Voraussetzungen für ihre Anordnung bestehen.

Das Land Baden-Württemberg hat die Verkehrsdatenabfrage als bislang letztes Bundesland eingeführt. § 23a PolG-BW trat im November 2008 in Kraft und ist bis zum 31.12.2012 befristet.

### *2.3 Bayern*

Das bayerische Polizeiaufgabengesetz (PAG) sieht in Art. 34b Abs. 2 Nr. 1, 2 i.V.m. Art. 34a Abs. 1 S. 1 die Möglichkeit einer präventiven Verkehrsdatenabfrage vor, sofern dies „zur Abwehr einer dringenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes, für Leib, Leben oder Freiheit einer Person oder für Sachen, soweit eine gemeine Gefahr besteht, erforderlich ist". Die Maßnahme darf sich gegen den für diese Gefahr Verant-

wortlichen richten sowie gegen Personen, die Nachrichten von oder für den Verantwortlichen übermitteln oder deren Kommunikationseinrichtungen der Verantwortliche verwendet.

Darüber hinaus enthält Art. 34b Abs. 2 i.V.m. Art. 34a Abs. 3 S. 1 Nr. 1 PAG-Bay eine spezielle Regelung für den Fall, dass sich die Maßnahme ausschließlich auf den Anschluss einer gefährdeten Person bezieht.

Welche Daten von einer Verkehrsdatenabfrage umfasst werden, wird in Art. 34b Abs. 3 PAG-Bay unter Bezugnahme auf § 113a TKG legaldefiniert. Deren Abfrage ist gem. Art. 34b Abs. 2 S. 2 PAG-Bay nur zulässig, wenn die Abwehr der drohenden Gefahr auf andere Weise aussichtslos oder wesentlich erschwert wäre. Ferner unterliegt sie gem. Art. 34c i.V.m. Art. 34 Abs. 4 S. 1, 2 PAG-Bay stets einem Richtervorbehalt. Bei Gefahr im Verzug kann die Maßnahme gem. Art. 34c Abs. 1 i.V.m. Art. 33 Abs. 5 S. 1, 2 PAG-Bay durch den Leiter eines Präsidiums der Landespolizei oder durch den Leiter des LKA angeordnet werden. Eine Übertragung dieser Anordnungsbefugnis auf Beamte des höheren Polizeivollzugsdienstes ist gem. Art. 34c Abs. 1 i.V.m. Art. 33 Abs. 5 S. 2 PAG-Bay möglich.

Die weitere Verwendung der durch die Verkehrsdatenabfrage erlangten Daten wird in Art. 34c PAG-Bay umfassend geregelt.

### *2.4 Hamburg*

In Hamburg ist eine Verkehrsdatenabfrage gem. § 10b Abs. 4 i.V.m. Abs. 1 i.V.m. § 10a Abs. 1 Hamburgisches Gesetz über die Datenverarbeitung der Polizei (HbgPolEDVG) zulässig, sofern dies zur Abwehr einer unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist. Sie darf sich nur gegen den für die Gefahr Verantwortlichen und einen Notstandspflichtigen i.S.d. § 10 Hamburgisches Gesetz zum Schutz der öffentlichen Sicherheit und Ordnung (HbgSOG) richten. Die unvermeidbare Betroffenheit Dritter steht der Maßnahme jedoch nicht entgegen.

Der Begriff der Verkehrsdaten wird in § 10b Abs. 5 HbgPolEDVG legaldefiniert.

Die Durchführung eines sog. Zielsuchlaufs[77] ist gem. § 10b Abs. 2 HbgPolEDVG nur zulässig wenn die Erforschung des Sachverhaltes auf andere Weise aussichtslos wäre. Er soll also nur als letztes Mittel, als *ultima ratio*, eingesetzt werden. Beschränkt sich die Verkehrsdatenabfrage hingegen auf die abgehenden Verbindungen des überprüften Anschlusses, ist ihr Einsatz nicht nur als *ultima ratio* zulässig.

In allen Fällen unterliegt die Verkehrsdatenabfrage auch in Hamburg einem Richtervorbehalt. Dieser ist in § 10c Abs. 1 HbgPolEDVG geregelt. Bei Gefahr im Vollzug kann die Maßnahme auch durch den Polizeipräsidenten angeordnet werden.

---

[77] Bei einem Zielsuchlauf wird darüber Auskunft verlangt, von welchem Anschluss aus Verbindungen auf dem überprüften Telefonanschluss eingegangen sind (vgl. Legaldefinition in § 10b Abs. 2 HbgPolEDVG). Er entspricht der sog. Zielwahlsuche gem. § 100g a.F. StPO.

*2.5 Hessen*

Eine eher knappe Regelung zur Verkehrsdatenabfrage befindet sich im hessischen Gesetz über die öffentliche Sicherheit und Ordnung (HSOG). Als einziges Landesgesetz, welches die Verkehrsdatenabfrage speziell regelt, nennt das HSOG an keiner Stelle den Begriff der Verkehrs- oder Verbindungsdaten. Gemäß § 15a Abs. 1 HSOG können die Polizeibehörden jedoch „von einem Dienstanbieter ... verlangen, dass er ... die näheren Umstände der Telekommunikation einschließlich des Standorts aktiv geschalteter nicht ortsfester Telekommunikationsanlagen übermittelt". Gemäß § 15a Abs. 2 HSOG „können die Polizeibehörden auch Auskunft über die Telekommunikation in einem zurückliegenden oder einem zukünftigen Zeitraum ... verlangen".

Ein derartiges Auskunftsverlangen ist gem. § 15a Abs. 1 HSOG zulässig, sofern dies zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person unerlässlich ist. Die Maßnahme bedarf gem. § 15a Abs. 5 HSOG außer bei Gefahr im Verzug einer richterlichen Anordnung. Besteht hingegen Gefahr im Verzug kann die Maßnahme gem. § 15a Abs. 5 S. 4 i.V.m. § 15 Abs. 5 S. 8, 9 HSOG auch von einer Polizeibehörde angeordnet werden. In diesem Fall muss eine richterliche Bestätigung unverzüglich, spätestens bis zum Ablauf des nächsten Tages eingeholt werden. Angaben zur weiteren Verwertung der erlangen Daten enthält § 15a Abs. 5 HSOG.

*2.6 Mecklenburg-Vorpommern*

In Mecklenburg-Vorpommern ist die Durchführung einer Verkehrsdatenabfrage gem. § 34a Abs. 5, 6 i.V.m. Abs. 1 Nr. 1, Abs. 2 Nr. 2 Gesetz über die öffentliche Sicherheit und Ordnung in Mecklenburg-Vorpommern (SOG M-V) immer dann zulässig, „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" und ohne sie die Erfüllung einer polizeilichen Aufgabe aussichtslos oder wesentlich erschwert wäre. Die Maßnahme darf sich nur gegen den für die Gefahr Verantwortlichen richten oder Daten des Gefährdeten selbst betreffen. Personenbezogene Daten Dritter dürfen gem. § 34a Abs. 1 S. 3 SOG M-V nur dann erhoben werden, wenn dies aus technischen Gründen unvermeidbar ist.

Gem. §§ 34a Abs. 4, 34 Abs. 3, 33 Abs. 3 SOG M-V bedarf die Verkehrsdatenabfrage einer richterlichen Anordnung, sofern sie sich auf die Verkehrsdaten aus einem Vertrauensverhältnis bezieht, welches durch ein Amts- oder Berufsgeheimnis i.S.d. §§ 53, 53a StPO geschützt ist. In allen anderen Fällen unterliegt sie keinem Richtervorbehalt.

Die Maßnahme ist gem. § 34a Abs. 4 S. 2 Hs. 2 SOG M-V auf höchstens drei Monate zu befristen. Solange die Voraussetzungen für ihre Anordnung vorliegen, kann sie jedoch um jeweils weitere drei Monate verlängert werden.

Schließlich enthält § 34a SOG M-V in den Absätzen 7 und 8 noch umfassende Reglungen zur Unterrichtung der Betroffenen und zur weiteren Verwendung der erlangten Daten.

### 2.7 *Niedersachsen*

In Niedersachsen darf eine Verkehrsdatenabfrage gem. § 33a Abs. 1, 2 Nr. 2, Abs. 7 Niedersächsisches Gesetz über die öffentliche Sicherheit und Ordnung (NdsSOG) durchgeführt werden, sofern dies zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist. Sie bedarf gem. § 33a Abs. 4 NdsSOG einer richterlichen Anordnung und ist auf höchstens drei Monate zu befristen. Solange die Voraussetzungen für eine Anordnung der Verkehrsdatenabfrage vorliegen, kann die Maßnahme – wie auch in Mecklenburg-Vorpommern – um jeweils drei weitere Monate verlängert werden. Bei Gefahr im Verzug ist gem. § 33a Abs. 5 NdsSOG der jeweilige Behördenleiter für die Anordnung der Verkehrsdatenabfrage zuständig. Dieser kann seine Anordnungsbefugnis wiederum auf Dienststellenleiter und auf Bedienstete des höheren Dienstes übertragen. Eine unvermeidbare Betroffenheit Dritter steht der Maßnahme gem. § 33a Abs. 2 S. 3 NdsSOG nicht entgegen. Die Telekommunikationsunternehmen werden durch § 33a Abs. 7 NdsSOG zur Mitwirkung an der Verkehrsdatenabfrage verpflichtet.

### *2.8 Rheinland-Pfalz*

§ 31 Abs. 1, 2 Nr. 2, Abs. 6 Polizei- und Ordnungsbehördengesetz Rheinland-Pfalz (RhPfPOG) lässt die Erhebung von Verkehrsdaten nur dann zu, wenn dies zur Abwehr einer gegenwärtigen Gefahr für Leib oder Leben einer Person zwingend erforderlich ist. Die Maßnahme darf sich gem. § 31 Abs. 2 S. 2 RhPfPOG nur auf Anschlüsse beziehen, die von einem Handlungsstörer, einem Zustandsstörer oder einem Notstandspflichtigen mit hoher Wahrscheinlichkeit genutzt werden oder von denen mit hoher Wahrscheinlichkeit eine Verbindung zu den genannten Personen hergestellt wird. Allerdings ist es gem. § 31 Abs. 2 S. 1 Hs. 2 RhPfPOG unschädlich, wenn Dritte von der Maßnahme unvermeidbar betroffen werden.

Besteht Gefahr im Verzug, kann die Verkehrsdatenabfrage in Rheinland-Pfalz gem. § 31 Abs. 5 RhPfPOG durch die Behördenleitung oder einen von ihr besonders beauftragten Beamten des höheren Dienstes angeordnet werden. In allen übrigen Fällen ist die Einholung einer richterlichen Anordnung erforderlich. Die Maßnahme ist auf drei Monate zu befristen, sie kann aber um jeweils weitere drei Monate verlängert werden, sofern die Voraussetzungen für ihre Anordnung vorliegen.

Die weitere Verwertung der durch die Verkehrsdatenabfrage erlangten Daten ist in § 31 Abs. 7, 8 i.V.m. § 29 Abs. 9 RhPfPOG geregelt.

### *2.9 Saarland*

Wie in Baden-Württemberg und Brandenburg ist eine Verkehrsdatenabfrage im Saarland gem. § 28b Abs. 1, 2 Saarländisches Polizeigesetz (SPolG) nicht nur zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person zulässig, sondern auch zur vorbeugenden Bekämpfung von schweren Straftaten. Dazu müssen konkrete Vorbereitungshandlungen, ggf. zusammen mit weiteren bestimmten Tatsachen, die begründete Annahme

rechtfertigen, dass eine der in § 100c StPO genannten Straftaten begangen werden soll. Allerdings nimmt § 28b Abs. 1 S. 2 SPolG die Bestechlichkeit i.S.d. § 332 StGB und die Bestechung i.S.d. § 334 StGB aus dem Anwendungsbereich der Verkehrsdatenabfrage heraus. In allen Fällen darf eine Verkehrsdatenabfrage jedoch nur durchgeführt werden, wenn die Erforschung des Sachverhaltes auf andere Weise aussichtslos oder wesentlich erschwert wäre.

Gemäß § 28b Abs. 5 SPolG unterliegt die Maßnahme auch im Saarland grundsätzlich einem Richtervorbehalt. Eine richterliche Anordnung ist gem. § 28b Abs. 5 S. 4 SPolG jedoch entbehrlich, wenn Gefahr im Verzug besteht. Ferner bedarf die Verkehrsdatenabfrage gem. § 28b Abs. 6 SPolG immer dann keiner richterlichen Anordnung, wenn die Maßnahme zum Zwecke der Gefahrenabwehr durchgeführt wird und ausschließlich der Ermittlung des Aufenthaltsortes einer Person dient. Erfolgt die Maßnahme hingegen zur vorbeugenden Bekämpfung einer Straftat i.S.d. § 28b Abs. 1 S. 1 Nr. 2 SPolG i.V.m. § 100c StPO muss sie von einem Richter angeordnet werden.

In allen Fällen, in denen die Verkehrsdatenabfrage keinem Richtervorbehalt unterliegt, kann sie gem. § 28b Abs. 5 S. 4, Abs. 6 SPolG von einem Behördenleiter oder einem von diesem besonders beauftragten Beamten des höheren Polizeivollzugsdienstes angeordnet werden.

§ 28 Abs. 7, 8 i.V.m. § 28a Abs. 5, 6 SPolG enthält Regelungen zum weiteren Verfahren und zur weiteren Verwendung der erlangten Daten. Besonders hervorzuheben ist, dass die Verkehrsdatenabfrage im Saarland gem. § 28 b Abs. 5 S. 2, 3 SPolG auf höchstens einen Monat zu befristen ist und sie, solange die Voraussetzungen für ihre Anordnung vorliegen, auch nur um jeweils einen Monat verlängert werden darf.

### *2.10 Schleswig-Holstein*

In Schleswig-Holstein ist die Verkehrsdatenabfrage im Landesverwaltungsgesetz (LVwG) geregelt. § 185a Abs. 4 i.V.m. Abs. 1, 2 Nr. 2 LVwG-SH setzt voraus, dass eine gegenwärtige Gefahr für Leib, Leben oder Freiheit einer Person besteht und die Maßnahme zur Aufklärung des Sachverhaltes unerlässlich ist. Sie darf sich gem. § 185a Abs. 1 S. 2 i.V.m. § 185 Abs. 2 S. 2 LVwG-SH nur gegen den für die Gefahr Verantwortlichen richten und gem. § 185a Abs. 3 S. 1 LVwG-SH nur solche Telefonanschlüsse erfassen, die von dem Verantwortlichen mit hoher Wahrscheinlichkeit genutzt werden oder von denen aus mit hoher Wahrscheinlichkeit Verbindung mit dem Verantwortlichen aufgenommen wird.

Die Mitwirkungspflicht der Telekommunikationsunternehmen bei der Erhebung der Verkehrsdaten ergibt sich aus § 185a Abs. 4 LVwG-SH. Detaillierte Regelungen zum Richtervorbehalt, der Eilkompetenz bei Gefahr im Verzug, zum weiteren Verfahren und zur Verwertung der erlangten Daten enthält § 186 LVwG-SH.

*2.11 Thüringen*

In Thüringen ist die Durchführung der Verkehrsdatenabfrage gem. §§ 34a Abs. 1 S. 1 Nr. 3, Abs. 3 Thüringisches Polizeiaufgabengesetz (PAG-Th) immer dann zulässig, 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 oder für Sachen, sofern eine gemeine Gefahr besteht, zwingend erforderlich ist. Darüber hinaus kann die Maßnahme durchgeführt werden, wenn konkrete Planungs- oder Vorbereitungshandlungen, ggf. zusammen mit weiteren Tatsachen, die begründete Annahme rechtfertigen, dass eine der in § 31 Abs. 5 PAG-Th numerisch aufgezählten Straftaten begangen werden soll. § 34a Abs. 3 S. 1 Nr. 2 PAG-Th nennt diverse Tatsachen, welche für die Planung einer Straftat sprechen.

Die Verkehrsdatenabfrage darf sich gegen den für die Gefahr Verantwortlichen und gegen den potentiellen Straftäter richten, sowie gegen all diejenigen Personen, welche Mitteilungen für diese Personen übermitteln oder deren Kommunikationseinrichtungen von den fraglichen Personen genutzt werden. Ferner ist die Erhebung von Daten Dritter gem. § 34a Abs. 3 S. 3 PAG-Th zulässig, sofern dies eine unvermeidliche Folge der Maßnahme darstellt.

Gem. § 34a Abs. 3 S. 1 PAG-Th darf eine Verkehrsdatenabfrage nur durchgeführt werden, wenn die Erfüllung einer polizeilichen Aufgabe ohne die Erkenntnisse aus dieser Maßnahme oder den damit verbundenen Maßnahmen wesentlich erschwert oder aussichtslos wäre. Sie bedarf gem. § 34a Abs. 5 PAG-Th einer richterlichen Anordnung, die nur der Leiter einer Polizeibehörde und bei dessen Verhinderung sein Stellvertreter beantragen dürfen. Selbige sind auch für die Anordnung der Maßnahme bei Gefahr in Verzug zuständig.

Hervorzuheben ist, dass sich die rückwirkende Verkehrsdatenabfrage gem. § 34a Abs. 3 S. 2 PAG-Th auf einen Zeitraum von maximal zwei Monaten beschränken muss.

*2.12 Andere Bundesländer*

In den Polizei- und Ordnungsgesetzen der Länder Berlin, Bremen, Nordrhein-Westfalen, Sachsen und Sachsen-Anhalt existiert bislang keine spezielle Ermächtigungsgrundlage für die Verkehrsdatenabfrage.

*2.13 Zusammenfassung*

Elf der 16 Bundesländer halten bislang eine spezielle Ermächtigungsgrundlage für Verkehrsdatenabfragen zu Zwecken der Gefahrenabwehr und Kriminalprävention bereit. Bei der Anwendung dieser Regelungen ist jedoch zu beachten, dass sich das Bundesverfassungsgericht im Rahmen seiner einstweiligen Anordnung zur Vorratsdatenspeicherung am 28. Oktober 2008[78] auch zur präventiven Verkehrsdatenabfrage geäußert hat. Danach sollen die angeforderten Verkehrsdaten zwecks Gefahrenabwehr gem. § 113b Nr. 2 TKG nur dann an die ersuchende Behörde übermittelt werden, wenn die Voraussetzungen der entsprechenden Ermäch-

[78] BVerfG, 1 BvR 256/08 vom 28.10.2008.

tigungsgrundlage vorliegen und die Verkehrsdatenabfrage zur Abwehr einer dringenden Gefahr für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder zur Abwehr einer dringenden Gefahr erforderlich ist.[79] Sind die zuletzt genannten Voraussetzungen nicht erfüllt, wohl aber die Voraussetzungen der die ersuchende Behörde zur Verkehrsdatenabfrage ermächtigenden Rechtsnorm, müssen die angeforderten Daten gleichwohl gespeichert werden.[80] Darüber hinaus weist das Bundesverfassungsgericht darauf hin, dass die Übermittlung von Verkehrsdaten nach § 113b Nr. 2 TKG außer bei Gefahr im Verzug stets einer richterlichen Anordnung bedarf.[81] In seinem Beschluss vom 22. April 2009[82] hat das Bundesverfassungsgericht die einstweilige Anordnung vom 28. Oktober 2008 für die Dauer von sechs Monaten, maximal bis zur Entscheidung in der Hauptsache, wiederholt. Der Termin für die mündliche Verhandlung ist auf den 15. Dezember 2009 anberaumt.

Allerdings bezieht sich die dargestellte Rechtsprechung des Bundesverfassungsgerichts ausschließlich auf die nach § 113a TKG gespeicherten Vorratsdaten. Diese dürfen gem. § 113b S. 1 TKG nur abgerufen werden, sofern die entsprechende Ermächtigungsgrundlage dies unter Bezugnahme auf § 113a TKG ausdrücklich vorsieht. Ein Abruf der Verkehrs- und Standortdaten i.S.d. §§ 96, 98 TKG wird von der dargestellten Rechtsprechung hingegen nicht erfasst und bedarf daher – vorbehaltlich abweichender Regelungen in den Landesgesetzen – bislang auch keiner richterlichen Anordnung.

Da nur die Länder Baden-Württemberg, Bayern, Schleswig-Holstein und Thüringen in ihrer Regelung zur Verkehrsdatenabfrage explizit auf § 113a TKG Bezug nehmen, dürfen die nach § 113a TKG gespeicherten Vorratsdaten auch nur in diesen Bundesländern abgerufen werden (vgl. § 113b S. 1 TKG). In allen anderen Bundesländern, so auch in Brandenburg, beschränkt sich die Verkehrsdatenabfrage auf die nach §§ 96, 98 TKG gespeicherten Daten, so dass die dargestellte Rechtsprechung des Bundesverfassungsgerichts dort nicht einschlägig ist.

### 3. Ortung von Mobiltelefonen

Von den drei Maßnahmen in der Evaluation finden sich für die Handyortung die meisten Spezialregelungen. 13 der 16 Bundesländer haben sie als Instrument der Gefahrenabwehr und Kriminalprävention in ihre Polizei- und Ordnungsgesetze aufgenommen. Dabei sind zahlreiche Parallelen zwischen den einzelnen landesrechtlichen Regelungen zu erkennen. So weisen alle Gesetze mit Ausnahme des hessischen Gesetzes über die öffentliche Sicherheit und Ordnung ausdrücklich darauf hin, dass die Maßnahme auch dann zulässig sein soll, wenn Dritte davon unvermeidbar betroffen werden. Diverse Parallelen sind ferner hinsichtlich der Vo-

---

[79] BVerfG, 1 BvR 256/08 vom 28.10.2008, Ls. 2 und Abs. 89 ff., 94 ff., 100; *Schenke*, S. 123, Rn. 197d.

[80] BVerfG, 1 BvR 256/08 vom 28.10.2008, Ls. 2.

[81] BVerfG, 1 BvR 256/08 vom 28.10.2008, Abs. 99 f.

[82] BVerfG, 1 BvR 256/08 vom 22.04.2009.

raussetzungen für die Handyortung erkennbar. Häufig wird sie im Zusammenhang mit der Verkehrsdatenabfrage geregelt, teilweise sind die Voraussetzungen für beide Maßnahmen sogar identisch. Dies ist im Hinblick auf den engen Sachzusammenhang auch naheliegend; es betrifft das telekommunikationstechnische Zusammenspiel beider Maßnahmen ebenso wie deren rechtliche Einordnung, welche beide Maßnahmen als gezielten Eingriff in das Recht auf informationelle Selbstbestimmung der betroffenen Personen erscheinen lässt.

### *3.1 Brandenburg*

**Denselben Voraussetzungen wie die Verkehrsdatenabfrage unterliegt die Handyortung zunächst im Land Brandburg. Gemäß § 33b Abs. 3 i.V.m. Abs. 1, 2 i.V.m. § 33a Abs. 1 BbgPolG kann die Polizei den Standort eines Mobiltelefons ermitteln, sofern dies zur Abwehr einer dringenden Gefahr für Leib, Leben oder Freiheit einer Person unerlässlich ist oder aufgrund tatsächlicher Anhaltspunkte davon auszugehen ist, dass eine der in § 33a Abs. 1 Nr. 2 BbgPolG numerisch aufgezählten Straftaten organisiert begangen werden soll. In letzterem Fall wird ferner vorausgesetzt, dass die drohende Rechtsgutsverletzung auch im konkreten Einzelfall schwer wiegt und die Verkehrsdatenabfrage zur Abwehr der durch diese Straftaten drohenden Gefahr erforderlich ist. Die Maßnahme darf sich gem. § 33b Abs. 3 Nr. 2 i.V.m. Abs. 2 BbgPolG nur gegen den für die Gefahr Verantwortlichen oder einen Notstandspflichtigen i.S.d. § 7 BbgPolG sowie gegen den potentiellen Straftäter und dessen Kontakt- oder Begleitpersonen richten. Letztere sind in § 33a Abs. 2 S. 3-5 genau definiert.**

**Anders als die Verkehrsdatenabfrage steht die Standortbestimmung nach § 33b Abs. 5 BbgPolG unter einem Richtervorbehalt, bei Gefahr im Verzug ist der jeweilige Behördenleiter für ihre Anordnung zuständig. § 33b Abs. 6 BbgPolG verpflichtet die Telekommunikationsunternehmen dazu, die Standortbestimmung zu ermöglichen.**

### *3.2 Baden-Württemberg*

Mit seiner im November 2008 in Kraft getretenen Regelung hat das Land Baden-Württemberg auch die Standortermittlung von Mobiltelefonen als bislang letztes Bundesland eingeführt. Sie unterliegt gem. § 23a Abs. 6 i.V.m. Abs. 1 PolG-BW denselben Voraussetzungen wie die Verkehrsdatenabfrage. Danach kann das Handy eines Handlungs- oder Zustandsstörers i.S.d. §§ 6, 7 PolG-BW sowie das von Notstandspflichtigen i.S.d. § 9 PolG-BW geortet werden, sofern dies zur Abwehr einer unmittelbar bevorstehenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leben, Gesundheit oder Freiheit einer Peron erforderlich ist. Zur vorbeugenden Bekämpfung von Straftaten i.S.d. § 23a Abs. 2 PolG-BW ist darüber hinaus die Standortermittlung des Mobiltelefons eines potentiellen Straftäters zulässig. Allerdings muss die geplante Straftat auch im konkreten Einzelfall schwer wiegen, und es müssen tatsächliche Anhaltspunkte dafür vorliegen, dass sie dem Bereich der terroristischen, der organisierten oder der Bandenkriminalität zuzuordnen ist. Ferner darf die Maßnahme gem. § 23a Abs. 6 i.V.m. Abs. 1 S. 3 PolG-BW nur durchgeführt werden,

wenn die Erfüllung der polizeilichen Aufgabe andernfalls gefährdet oder wesentlich erschwert wäre.

Einem Richtervorbehalt unterliegt die Handyortung in Baden-Württemberg nicht. Stattdessen muss sie gem. § 23a Abs. 6 S. 3 i.V.m. § 22 Abs. 6 PolG-BW von einem Regierungspräsidenten, dem Leiter des LKA, eines Polizeipräsidiums oder einer Polizeidirektion angeordnet werden. Die Regierungspräsidenten, der Leiter des LKA und die Leiter der Polizeipräsidien können ihre Anordnungsbefugnis jedoch auf besonders beauftragte Beamte des höheren Dienstes übertragen.

*3.3 Bayern*

In Bayern richtet sich die Zulässigkeit einer Handyortung nach § 34a Abs. 2 S. 1 Nr. 2 i.V.m. Abs. 1 PAG-Bay. Sie ist zulässig, wenn dies zur Abwehr einer dringenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes, für Leib, Leben oder Freiheit einer Person oder für Sachen, soweit eine gemeine Gefahr besteht, erforderlich ist. Sie darf sich gegen den für diese Gefahr Verantwortlichen selbst richten, gegen Personen die für ihn Nachrichten übermitteln, sowie gegen Personen, deren Kommunikationseinrichtungen er verwendet. Ferner muss die Erfüllung polizeilicher Aufgaben ohne die Standortermittlung aussichtslos sein oder wesentlich erschwert werden. Eine Mitwirkungspflicht der Telekommunikationsunternehmen ergibt sich dabei aus § 34b Abs. 2 S. 1 Nr. 3 PAG-Bay.

Für den Fall, dass eine Gefahr für Leben oder Gesundheit einer Person besteht, hält § 34a Abs. 3 S. 1 Nr. 2 PAG-Bay eine Sonderregelung bereit. Danach darf der Standort eines Mobiltelefons, welches die gefährdete Person bei sich führt, auch dann ermittelt werden, wenn die strengen Voraussetzungen des § 34a Abs. 1 PAG-Bay nicht vorliegen.

Das Verfahren und die Verwendung der erlangten Daten sind in § 34c PAG-Bay umfassend geregelt. Aus § 34c Abs. 1 i.V.m. § 34 Abs. 4 PAG-Bay ergibt sich, dass die Maßnahme einer richterlichen Anordnung bedarf. Bei Gefahr im Verzug sind gem. § 34c Abs. 1 i.V.m. § 33 Abs. 5 PAG-Bay der Leiter eines Präsidiums der Landespolizei und der Leiter des LKA anordnungsbefugt. Sie können diese Eilkompetenz jedoch auf Beamte des höheren Polizeivollzugsdienstes übertragen. Wird gem. § 34a Abs. 3 S. 1 Nr. 2 PAG-Bay nur das Mobiltelefon einer gefährdeten Person geortet, entfällt der Richtervorbehalt. Die Anordnungsbefugnis liegt in diesem Fall gem. § 34c Abs. 2 PAG-Bay i.V.m. § 4 Abs. 2 S. 1 Nr. 1, 2 POG-Bay bei den Dienststellenleitern der Präsidien, der Inspektionen und der Kriminalfachdezernate sowie bei dem Leiter des LKA. Diese können ihre Anordnungsbefugnis auf besonders Beauftragte übertragen.

*3.4 Berlin*

Obwohl die Verkehrsdatenabfrage im Allgemeinen Sicherheits- und Ordnungsgesetz des Landes Berlin nicht vorgesehen ist, enthält § 25a Abs. 1, 2 ASOG Bln eine spezielle Regelung zur Handyortung. Sie ist immer dann zulässig, wenn eine gegenwärtige Gefahr für Leib oder Leben einer Person besteht und „die Ermittlung des Aufenthaltsortes einer vermissten, suizidgefährdeten oder einen Notruf auslösenden gefährdeten hilflosen Person auf andere

Weise aussichtslos oder wesentlich erschwert wäre". Allerdings darf gem. § 25a Abs. 2 ASOG Bln ausschließlich der Standort desjenigen Mobiltelefons ermittelt werden, welches von der „vermissten, suizidgefährdeten oder einen Notruf auslösenden gefährdeten hilflosen Person" mitgeführt wird.

Einer richterlichen Anordnung bedarf die Maßnahme nach dem ASOG Bln nicht. Vielmehr sind gem. § 25a Abs. 2 ASOG Bln die Polizei und die Feuerwehr für die Standortermittlung zuständig. Die Telekommunikationsunternehmen werden durch § 25a Abs. 1 ASOG Bln zur Übermittlung der entsprechenden Daten verpflichtet.

Zusammenfassend muss daher festgehalten werden, dass das ASOG Bln zwar keine spezielle Regelung zur Verkehrsdatenabfrage insgesamt bereithält, die Polizei und die Feuerwehr in § 25a Abs. 1 ASOG Bln aber doch zur Abfrage einzelner Verkehrsdaten – den Standortdaten eines von einer gefährdeten Person mitgeführten Mobiltelefons – ermächtigt. Die Standortermittlung wird zwar in § 25a Abs. 2 ASOG Bln speziell geregelt, gleichzeitig aber ebenfalls auf diejenigen Mobiltelefone beschränkt, welche eine gefährdete Person bei sich führt. Somit haben beide Maßnahmen nach dem ASOG Bln nur einen sehr engen Anwendungsbereich.

### *3.5 Bremen*

Ein weiteres Bundesland, welches die Verkehrsdatenabfrage nicht, wohl aber die Standortermittlung speziell regelt, ist das Land Bremen. Gem. § 33 Abs. 1 S. 1 i.V.m. § 32 Abs. 1 S. 1 Nr. 1 - 3 Bremer Polizeigesetz (BremPolG) ist die Ermittlung des Aufenthaltsortes eines Handlungs- oder Zustandsstörers i.S.d. §§ 5, 6 BremPolG zulässig, wenn dies zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit erforderlich erscheint. Ferner darf der Aufenthaltsort von solchen Personen bestimmt werden, bei denen Tatsachen die Annahme rechtfertigen, dass sie Straftaten von erheblicher Bedeutung begehen werden. In beiden Fällen muss die polizeiliche Aufgabenerfüllung ohne die Standortermittlung unmöglich erscheinen. Unter eng begrenzten Voraussetzungen kann darüber hinaus der Standort von Kontakt- oder Begleitpersonen des potentiellen Straftäters ermittelt werden. Einer richterlichen Anordnung bedürfen die Maßnahmen nach § 33 BremPolG nicht.

### *3.6 Hamburg*

Gem. § 10b Abs. 3 S. 1 Nr. 2, S. 3 HbgPolEDVG darf „zur Abwehr einer unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person der Standort eines aktiv geschalteten Mobilfunkendgerätes ermittelt werden", sofern „die Ermittlung des Aufenthaltsortes auf andere Weise weniger Erfolg versprechend oder erschwert" wäre. Die Maßnahme unterliegt gem. § 10c Abs. 1 HbgPolEDVG einem Richtervorbehalt, sie kann bei Gefahr im Verzug jedoch durch den Polizeipräsidenten angeordnet werden. Darüber hinaus enthält § 10c HbgPolEDVG weitere Verfahrensvorschriften. Eine Mitwirkungspflicht der Telekommunikationsunternehmen ergibt sich aus § 10b Abs. 4 S. 1 Nr. 3, S. 2 HbgPolEDVG.

*3.7 Hessen*

Auch in Hessen ist die Standortermittlung gem. § 15a Abs. 3 HSOG zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person zulässig. Sie bedarf gem. § 15a Abs. 5 HSOG außer bei Gefahr im Verzug einer richterlichen Anordnung. Die hessische Regelung ist die einzige ihrer Art, welche nicht ausdrücklich darauf hinweist, dass eine Standortermittlung auch dann zulässig ist, wenn Dritte unvermeidbar betroffen sind. Es wird im weiteren Verlauf der Evaluation noch zu prüfen sein, ob nicht auch die hessische Regelung in dieser Weise auszulegen wäre.

*3.8 Mecklenburg-Vorpommern*

Im Mecklenburg-Vorpommern sind die Standortermittlung und die Verkehrsdatenabfrage einheitlich in § 34a SOG M-V geregelt und unterliegen denselben Voraussetzungen. Gem. § 34a Abs. 1, 2 Nr. 3 SOG M-V darf der Standort eines Mobiltelefons ermittelt werden, wenn eine Gefahr für Leib, Leben oder Freiheit einer Person oder für den Bestand oder die Sicherheit des Bundes oder eines Landes besteht und die Maßnahme zur Abwehr dieser Gefahr erforderlich ist. Sie darf sich nur auf das Handy des für die Gefahr Verantwortlichen, bei einer Gefahr für Leben oder Gesundheit einer Person auch auf das Mobiltelefon der gefährdeten Person beziehen. Ferner darf die Maßnahme nur durchgeführt werden, wenn ohne sie die Erfüllung einer polizeilichen Aufgabe aussichtslos oder wesentlich erschwert wäre.

Grundsätzlich unterliegt die Standortermittlung in Mecklenburg-Vorpommern keinem Richtervorbehalt. Nur wenn sie sich auf ein Vertrauensverhältnis bezieht, welches durch ein Amts- oder Berufsgeheimnis i.S.d. §§ 53, 53a StPO geschützt ist und keine Gefahr im Verzug besteht, ist eine richterliche Anordnung gem. §§ 34a Abs. 3, 34 Abs. 3, 33 Abs. 6 SOG M-V erforderlich. Die Maßnahme ist gem. § 34a Abs. 4 S. 2 Hs. 2 SOG M-V auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils drei Monate ist gem. § 34a Abs. 4 S. 3 SOG M-V möglich, solange die Voraussetzungen des § 34a Abs. 1 SOG M-V vorliegen. Diese Regelungen zur Befristung gelten für alle nach § 34a Abs. 1, 3 SOG M-V zulässigen Maßnahmen und damit auch für die Ortung von Mobiltelefonen. Es ist jedoch davon auszugehen, dass die Befristung ihm Rahmen der Handyortung kaum von praktischer Relevanz ist. Diese Maßnahme stellt sich in aller Regel als eine Maßnahme von kurzer Dauer dar, sodass bereits der im Gesetz vorgesehene dreimonatige Regelzeitraum kaum auch nur ansatzweise ausgeschöpft werden dürfte.

In den Absätzen 7 und 8 enthält § 34a SOG M-V umfassende Regelungen zum Verfahren und zur Verwendung der erlangten Daten. Eine Verpflichtung der Telekommunikationsunternehmen, die Standortermittlung zu ermöglichen, ergibt sich aus § 34a SOG M-V.

*3.9 Niedersachsen*

Das niedersächsische Sicherheits- und Ordnungsgesetz regelt die Verkehrsdatenabfrage und die Standortermittlung ebenfalls einheitlich. Gem. § 33a Abs. 1, 2 Nr. 3 NdsSOG ist also

auch die Standortermittlung eines Mobiltelefons zulässig, wenn dies zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist.[83]

Der Richtervorbehalt gem. § 33a Abs. 4 NdsSOG unterliegt zwei wichtigen Ausnahmen. Besteht Gefahr im Verzug, so kann die Maßnahme gem. § 33a Abs. 5 NdsSOG von dem jeweiligen Behördenleiter angeordnet werden, der diese Anordnungsbefugnis wiederum auf Dienststellenleiter und auf Bedienstete des höheren Dienstes übertragen kann. Ferner bedarf die Standortermittlung gem. § 33a Abs. 6 NdsSOG auch dann keiner richterlichen Anordnung, wenn sie „ausschließlich der Ermittlung des Aufenthaltsortes der gefährdeten Person" dient.

Gem. § 33a Abs. 4 S. 2 Hs. 2, S. 3 NdsSOG ist die Standortermittlung auch in Niedersachsen auf höchstens drei Monate zu befristen. Solange die Voraussetzungen für ihre Anordnung vorliegen, kann die Maßnahme jedoch um jeweils weitere drei Monate verlängert werden. Zur praktischen Relevanz dieser Regelung gilt auch hier das oben Gesagte. Die Telekommuni-kationsunternehmen werden durch § 33a Abs. 7 NdsSOG dazu verpflichtet, die Durchführung der Maßnahme zu ermöglichen.

### *3.10 Rheinland-Pfalz*

Auch Rheinland-Pfalz hat eine einheitliche Regelung für Verkehrsdatenabfrage und Standortermittlung implementiert. Die Standortermittlung darf daher gem. § 31 Abs. 1, 2 S. 1 Nr. 3 RhPfPOG durchgeführt werden, wenn dies zur Abwehr einer gegenwärtigen Gefahr für Leib oder Leben einer Person zwingend erforderlich ist. Sie muss sich jedoch gem. § 31 Abs. 2 S. 2 RhPfPOG auf diejenigen Mobiltelefone beschränken, welche von einem Handlungsstörer, einem Zustandsstörer oder einem Notstandspflichtigen mit hoher Wahrscheinlichkeit genutzt werden oder von denen mit hoher Wahrscheinlichkeit eine Verbindung zu den genannten Personen hergestellt wird.

Während die Maßnahme grundsätzlich einer richterlichen Anordnung bedarf, kann sie bei Gefahr im Verzug gem. § 31 Abs. 5 RhPfPOG durch die Behördenleitung angeordnet werden. Diese kann ihre Eilkompetenz auf einen besonders beauftragten Beamten des höheren Dienstes übertragen. Auch in Rheinland-Pfalz erstreckt sich aufgrund der gemeinsamen Regelungstechnik die Befristungsregelung der Verkehrsdatenabfrage auf die Standortermittlung (zunächst drei Monate mit entsprechenden Verlängerungsmöglichkeiten, solange die Voraussetzungen für ihre Anordnung fortbestehen). Auch hier gilt das oben Gesagte entsprechend.

Die Telekommunikationsunternehmen werden durch § 31 Abs. 6 RhPfPOG zur Mitwirkung verpflichtet. Regelungen zur weiteren Verwertung der erlangten Daten befinden sich in § 31 Abs. 7, 8 i.V.m. § 29 Abs. 9 RhPfPOG.

---

[83] *Böhrenz / Siefken*, § 33a Rn. 5.

*3.11 Saarland*

Obwohl § 28b SPolG explizit nur von der Erhebung personenbezogener Informationen durch die Überwachung und Aufzeichnung der Telekommunikation spricht, ist davon auszugehen, dass auch die Standortermittlung von diese Regelung erfasst wird. § 28b Abs. 2 SPolG verpflichtet die Telekommunikationsunternehmen u.a. dazu, bei Anordnung einer Maßnahme nach Absatz 1 Informationen zum Standort eines Mobiltelefons zu erteilen. Da die Telekommunikationsunternehmen jedoch nur wissen, in welcher Funkzelle sich ein Mobiltelefon befindet, und den Standort eines Mobiltelefons daher nur sehr grob festlegen können, wären die nach § 28b Abs. 2 SPolG zu erteilenden Informationen für die Polizei praktisch bedeutungslos, wenn sich der Abfrage von Standortdaten keine genauere Ortung mit eigenen Mitteln anschließen dürfte. Eine Gesamtschau des § 28b SPolG führt also zu der Annahme, dass sein Absatz 1 auch zur Ortung von Mobiltelefonen ermächtigt. Dieses Ergebnis widerspricht auch nicht dem ausdrücklichen Wortlaut des § 28b Abs. 1 SPolG, sofern man davon ausgeht, dass es sich bei den Standortdaten um personenbezogene Informationen handelt und die Ortung als eine Form der Telekommunikationsüberwachung im Sinne dieser Vorschrift einzuordnen ist.

Auf der Basis einer solchen Auslegung des § 28b Abs. 1 SPolG dürfte eine Standortermittlung im Saarland also zulässig sein, sofern dies zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person oder zur vorbeugenden Bekämpfung einer der in § 100c StPO genannten Straftaten mit Ausnahme der Bestechlichkeit i.S.d. § 332 StGB und der Bestechung i.S.d. § 334 StGB erforderlich ist und die Erforschung des Sachverhaltes auf andere Weise aussichtslos oder wesentlich erschwert wäre.

Ähnlich der niedersächsischen Regelung macht auch das saarländische Polizeigesetz von dem gem. § 28b Abs. 5 S. 1 SPolG grundsätzlich bestehenden Richtervorbehalt zwei Ausnahmen: § 28b Abs. 5 S. 4 SPolG sieht von dem Erfordernis einer richterlichen Anordnung ab, wenn Gefahr im Verzug besteht. Darüber hinaus ist eine richterliche Anordnung gem. § 28b Abs. 6 SPolG entbehrlich, wenn die Standortermittlung der Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person i.S.d. § 28b Abs. 1 S.1 Nr. 1 SPolG dient. Im Ergebnis unterliegt die Handyortung nach dem saarländischen Polizeigesetz also nur dann einem Richtervorbehalt, wenn sie zur vorbeugenden Bekämpfung einer Straftat i.S.d. § 28b Abs. 1 S. 1 Nr. 2 SPolG durchgeführt wird.

In allen Fällen, in denen die Maßnahme keiner richterlichen Anordnung bedarf, kann sie gem. § 28b Abs. 5 S. 4 bzw. Abs. 6 S. 1, 2 SPolG durch einen Behördenleiter oder einen von diesem besonders beauftragten Beamten des höheren Polizeivollzugsdienstes angeordnet werden.

In § 28 Abs. 7, 8 i.V.m. § 28a Abs.5, 6 SPolG befinden sich weitere Regelungen zum Verfahren und zur Verwendung der durch die Maßnahme erlangen Daten. Wie in vielen anderen Bundesländern ist die Standortermittlung auch im Saarland zu befristen. Einzigartig ist jedoch, dass die Frist gem. § 28b Abs. 5 S. 2, 3 SPolG höchstens einen Monat beträgt und die Maßnahme, solange die Voraussetzungen für ihre Anordnung vorliegen, auch nur um jeweils einen Monat verlängert werden darf.

*3.12 Schleswig-Holstein*

In Schleswig-Holstein darf der Standort eines Mobiltelefons gem. § 185a Abs. 1, 2 Nr. 3 LVwG-SH ermittelt werden, sofern dies zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person unerlässlich ist. Die Maßnahme darf sich gem. § 185a Abs. 1 S. 2 i.V.m. § 185 Abs. 2 S. 2 LVwG-SH nur gegen den für die Gefahr Verantwortlichen richten und gem. § 185a Abs. 3 S. 1 LVwG-SH nur diejenigen Mobiltelefone erfassen, welche von dem für die Gefahr Verantwortlichen mit hoher Wahrscheinlichkeit genutzt werden oder von denen aus mit ihm mit hoher Wahrscheinlichkeit Verbindung aufgenommen wird.

Eine Mitwirkungspflicht der Telekommunikationsunternehmen ergibt sich aus § 185a Abs. 4 LVwG-SH. Umfassende Regelungen zum Richtervorbehalt, der Eilkompetenz bei Gefahr im Verzug, zum weiteren Verfahren und zur Verwertung der erlangten Daten befinden sich in § 186 LVwG-SH.

*3.13 Thüringen*

In Thüringen bestimmt sich die Zulässigkeit der Standortermittlung eines Mobiltelefons schließlich nach § 34a Abs. 2 S. 1 Nr. 3, Abs. 3 S. 1 PAG-Th. Danach ist die Maßnahme zulässig, sofern sie 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, sofern eine gemeine Gefahr besteht, zwingend erforderlich ist. Darüber hinaus kann die Maßnahme durchgeführt werden, wenn konkrete Planungs- oder Vorbereitungshandlungen, ggf. zusammen mit weiteren Tatsachen, die begründete Annahme rechtfertigen, dass eine der in § 31 Abs. 5 PAG-Th numerisch aufgezählten Straftaten begangen werden soll. Welche Tatsachen für die Planung einer entsprechenden Straftat sprechen, beschreibt § 34a Abs. 3 S. 1 Nr. 2 PAG-Th mit Hilfe einer weiteren numerischen Aufzählung sehr genau.

Zielpersonen können gem. § 34a Abs. 3 PAG-Th in erster Linie der für die Gefahr Verantwortliche und die potentiellen Straftäter sein. Darüber hinaus kann sich die Maßnahme aber auch gegen Personen richten, die Mitteilungen für den Gefahrverantwortlichen bzw. einen Straftäter übermitteln oder deren Kommunikationseinrichtungen von diesen genutzt werden. Sie darf gem. § 34a Abs. 3 S. 1 PAG-Th nur dann durchgeführt werden, wenn die Erfüllung einer polizeilichen Aufgabe ohne die Erkenntnisse aus dieser Maßnahme oder den damit verbundenen Maßnahmen wesentlich erschwert oder aussichtslos wäre.

Gemäß § 34a Abs. 5 PAG-Th bedarf die Standortermittlung auch in Thüringen einer richterlichen Anordnung. Einen entsprechenden Antrag dürfen nur der Leiter einer Polizeibehörde und bei dessen Verhinderung sein Stellvertreter stellen. Selbige sind auch für die Anordnung der Maßnahme bei Gefahr im Verzug zuständig.

### *3.14 Andere Bundesländer*

Keine spezielle Regelung zur Handyortung sehen die Polizei- und Ordnungsgesetze der Länder Nordrhein-Westfahlen, Sachsen und Sachsen-Anhalt vor.

### *3.15 Zusammenfassung*

Die Gegenüberstellung der einzelnen landesrechtlichen Regelungen zur Standortermittlung einerseits und zur Verkehrsdatenabfrage andererseits macht deutlich, dass beide Maßnahmen in der Regel ähnlichen Voraussetzungen unterliegen oder gar einheitlich geregelt sind – vorausgesetzt beide Maßnahmen sind in dem jeweiligen Landesrecht speziell geregelt.

Deutliche Unterschiede sind jedoch hinsichtlich der Anordnungsbefugnis zu verzeichnen. Während die Verkehrsdatenabfrage in den meisten Bundesländern einem Richtervorbehalt unterliegt, ist eine richterliche Anordnung der Standortermittlung nur in sieben Bundesländern immer erforderlich. In zwei weiteren Bundesländern (Niedersachsen, Saarland) besteht für die Standortermittlung zwar grundsätzlich auch ein Richtervorbehalt, dieser wird aber in bestimmten Fällen durchbrochen. Drei Bundesländer (Baden-Württemberg, Berlin und Bremen) sehen von einer richterlichen Anordnung vollständig ab, in Mecklenburg-Vorpommern ist sie nur in Einzelfällen erforderlich.

Festzuhalten ist, dass sich die Handyortung von den drei auf dem Prüfstand stehenden Maßnahmen am stärksten durchgesetzt hat und am weitesten verbreitet ist: Lediglich drei Bundesländer haben diese Maßnahme in ihren Polizei- und Ordnungsgesetzen bislang nicht speziell geregelt. Allerdings bleibt abzuwarten, ob die ausstehenden Gesetzesänderungen[84] dieses Bild verändern oder bestätigen werden.

## 4. Automatische Kennzeichenfahndung

Von den drei hier zu prüfenden Maßnahmen wird die automatische Kennzeichenfahndung gegenwärtig wohl am kontroversesten diskutiert. Dies liegt v.a. darin begründet, dass sie sich nach Wahrnehmung der Kritiker nicht nur speziell gegen Polizeipflichtige und potentielle Straftäter, sondern gegen die „Gesamtheit der Autofahrer" richtet, was durch terminologische Verweise auf „systematische Kontrollen" und „Kfz-Massenabgleiche" noch unterstrichen wird.[85] Darüber hinaus wird die öffentliche Diskussion dadurch geprägt, dass das Bundesverfassungsgericht die Regelungen zur automatischen Kennzeichenfahndung bislang in zwei

---

[84] Vgl. Fn. 76.

[85] Vgl. Pressemitteilung von DatenSpeicherung.de, 30.10.2009, siehe http://www.daten-speicherung.de/index.php/urteil-zu-kfz-massenabgleich-in-bayern-veroeffentlicht/; SpiegelOnline, 28.07.2009, siehe: http://www.spiegel.de/politik/deutschland/0,1518,638526,00.html (15.03.2011).

Bundesländern für verfassungswidrig erklärt hat[86] und ein vom ADAC in Auftrag gegebenes Gutachten keine einzige Landesregelung als vollkommen zufriedenstellend erachtet.[87]

Diese allgemeine Skepsis gegenüber der automatischen Kennzeichenfahndung hat sicherlich mit dazu beigetragen, dass sie von den hier zu evaluierenden Maßnahmen diejenige ist, welche bislang am wenigsten verbreitet ist. Während die Verkehrsdatenabfrage bereits in elf und die Handyortung sogar in 13 Bundesländern implementiert wurden, ist die automatische Kennzeichenfahndung als präventiv-polizeiliche Maßnahme derzeit nur in zehn Bundesländern speziell geregelt. Die einschlägigen Normen werden im Folgenden ebenfalls gegenübergestellt, auch hier ohne eine abschließende inhaltliche Bewertung vorzunehmen. Dies gilt insbesondere für die Regelung in Brandenburg, die in diesem frühen Projektstadium noch nicht kommentiert werden soll. Dies muss umso mehr gelten, als die Evaluation der auf der Grundlage von § 36a BbgPolG tatsächlich durchgeführten Maßnahmen noch aussteht.

### *4.1 Brandenburg*

**Gem. § 36a BbgPolG ist die Durchführung einer anlassbezogenen automatischen Kennzeichenfahndung zulässig, sofern sie zur Abwehr einer gegenwärtigen Gefahr für Leib oder Leben einer Person oder zur Abwehr einer sonstigen Gefahr erforderlich ist und in letzterem Fall die Voraussetzungen für eine Identitätsfeststellung nach § 12 Abs. 1 Nr. 2-4 BbgPolG vorliegen. Ferner kann eine automatische Kennzeichenfahndung durchgeführt werden, wenn eine Person oder ein Fahrzeug nach § 36 Abs. 1, 1a BbgPolG polizeilich ausgeschrieben wurde und Tatsachen die Annahme rechtfertigen, dass die für die Ausschreibung relevante Begehung von Straftaten unmittelbar bevorsteht.**

**Ob die Maßnahme nur offen oder auch in verdeckter Form durchgeführt werden darf, ist in § 36a BbgPolG nicht geregelt.**

**Gem. § 36a Abs. 2 BbgPolG können die erhobenen Daten mit denjenigen Daten automatisch abgeglichen werden, welche zur Abwehr dieser Gefahren gespeichert wurden. Im Trefferfall können die Daten gem. § 36a Abs. 2 S. 2 BbgPolG polizeilich verarbeitet und ggf. weitere Maßnahmen eingeleitet werden. Liegt kein Trefferfall vor, sind die Daten gem. § 36a Abs. 2 S. 3 BbgPolG unverzüglich zu löschen.**

### *4.2 Baden-Württemberg*

Baden-Württemberg hat die automatische Kennzeichenfahndung im November 2008 als bislang letztes Bundesland in sein Polizeigesetz aufgenommen. Gemäß § 22a Abs. 1 S. 1 PolG-BW kann der Polizeivollzugsdienst „zur Abwehr einer Gefahr oder zur vorbeugenden Bekämpfung von Straftaten bei Kontrollen nach § 26 Abs. 1 [...] Bilder von Fahrzeugen aufzeichnen und deren Kennzeichen ermitteln". Mit seinem Verweis auf § 26 Abs. 1 PolG-BW

---

86 BVerfG, 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008.

87 Siehe zusammenfassend *Roßnagel* (Verfassungsrechtliche Bewertung), S. 87 f.

nimmt die Vorschrift Bezug auf die Personenfeststellung, welche nur unter bestimmten, numerisch aufgezählten Voraussetzungen durchgeführt werden darf. Danach ist die Maßnahme insbesondere an Orten zulässig, an denen erfahrungsgemäß Straftaten verabredet, vorbereitet oder verübt werden (Nr. 2), an besonders gefährlichen Orten (Nr. 3), an Kontrollstellen (Nr.4) oder in einem Kontrollbereich i.S.d. § 26 Abs. 1 Nr. 4, 5 PolG-BW.

Die auf diese Weise ermittelten Kennzeichen dürfen gem. § 22a Abs. 2 PolG-BW automatisch mit dem Fahndungsbestand der Sachfahndungsdatei des polizeilichen Informationssystems abgeglichen werden. Dieses polizeiliche Informationssystem wird nach den Vorschriften des BKA-Gesetzes beim BKA geführt. § 22a Abs. 2 S. 2 PolG-BW weist ferner darauf hin, dass es auch diejenigen Kennzeichen enthält, welche im Schengener Informationssystem ausgeschrieben sind. Allerdings beschränkt § 22a Abs. 2 S. 3 PolG-BW den Abgleich auf die Kennzeichen solcher Fahrzeuge, die zur polizeilichen Beobachtung, zur Registrierung, zur gezielten Kontrolle (Nr. 1), auf Grund einer erheblichen Gefahr zu deren Abwehr (Nr. 2), auf Grund des Verdachts einer Straftat für Zwecke der Strafverfolgung (Nr. 3) oder aus Gründen der Strafverfolgung (Nr. 4) ausgeschrieben sind.

Gem. § 22a Abs. 1 S. 2 PolG-BW darf die Bildaufzeichnung auch dann erfolgen, wenn Insassen der Fahrzeuge unvermeidbar betroffen werden. Ihr flächendeckender Einsatz ist gem. § 22a Abs. 2 S. 3 PolG-BW jedoch nicht zulässig, längerfristig oder gar dauerhaft darf die Maßnahme nur in bestimmten Fällen durchgeführt werden. Des Weiteren schließt § 22a Abs. 2 S. 4 PolG-BW einen Abgleich mit Kennzeichenfragmenten aus; es müssen also stets die vollständigen Kennzeichen abgeglichen werden. Liegt keine Übereinstimmung mit dem Fahndungsbestand vor, sind die erfassten Kennzeichen gem. § 22a Abs. 3 PolG-BW unverzüglich nach dem Abgleich zu löschen. Führt der Abgleich hingegen zu einem Trefferfall, dürfen gem. § 22a Abs. 4 PolG-BW das Kennzeichen, das angefertigte Bild sowie Angaben zu Ort, Fahrtrichtung, Datum und Uhrzeit gespeichert werden. Ferner dürfen das Fahrzeug angehalten und nach einer Überprüfung des Trefferfalls weitere Maßnahmen eingeleitet werden.

Obwohl § 22a Abs. 1 PolG-BW lediglich vom „verdeckten Einsatz" dieser Maßnahme spricht, wird eine offen durchgeführte Kennzeichenfahndung als weniger einschneidende Maßnahme ebenfalls für zulässig erachtet.[88]

Im November 2009 wurde gegen die baden-württembergische Regelung zur automatischen Kennzeichenfahndung in § 22a PolG-BW Verfassungsbeschwerde eingelegt.[89]

---

[88] *Belz/Mußmann*: Polizeigesetz für Baden-Württemberg, 7. Auflage (2009), § 22a Rn. 8 i.V.m. § 19 Rn. 24; *Wolf/Stephan/Deger*: Polizeigesetz für Baden-Württemberg, 6. Auflage (2009), § 22a Rn. 2 i.V.m. § 19 Rn. 10.

[89] http://www.daten-speicherung.de/data/Beschwerdeschrift_Kfz-Massenscanning_BW_2009-11-13.pdf; siehe auch http://www.auto-motor-und-sport.de/news/kennzeichen-scan-autofahrer-klagen-gegen-abgleich-von-autonummern-1491186.html; http://www.golem.de/0911/71540.html; http://www.heise.de/newsticker/meldung/Verfassungsbeschwerde-gegen-Kfz-Scanning-in-Baden-Wuerttemberg-872035.html (15.03.2011).

*4.3 Bayern*

In Bayern darf eine automatische Kennzeichenfahndung gem. Art. 33 Abs. 2 S. 2 PAG-Bay immer dann durchgeführt werden, wenn die Voraussetzungen für eine Identitätsfeststellung i.S.d. Art. 13 Abs. 1 Nr. 1 - 5 PAG-Bay vorliegen. Somit ist sie zu jeder Zeit im Grenzgebiet, auf Durchgangsstraßen und an gefährlichen oder gefährdeten Orten der in Art. 13 Abs. 1 Nr. 2, 3 PAG-Bay umschriebenen Art zulässig. Ferner darf eine automatische Kennzeichenfahndung durchgeführt werden, wenn eine Kontrollstelle i.S.d. Art. 13 Abs. 1 Nr. 4 PAG-Bay rechtmäßig errichtet wurde oder wenn die Maßnahme zur Abwehr einer Gefahr erforderlich ist.

Soll die automatische Kennzeichenfahndung verdeckt durchgeführt werden, muss die Erfüllung polizeilicher Aufgaben auf andere Weise gem. Art. 33 Abs. 2 S. 2 i.V.m. Art. 30 Abs. 3 S. 2 PAG-Bay gefährdet oder erheblich erschwert sein.

Mit welchen polizeilichen Fahndungsbeständen die erfassten Kennzeichen abgeglichen werden dürfen, wird in Art. 33 Abs. 2 S. 3 PAG-Bay genau dargelegt. Hervorzuheben ist, dass auch ein Abgleich mit polizeilichen Fahndungsbeständen über gestohlene oder sonst abhanden gekommene Fahrzeuge zulässig ist. Nach dem Abgleich müssen die erhobenen Daten – gem. Art. 33 Abs. 2 S. 2 PAG-Bay also das jeweilige Kennzeichen, die Fahrtrichtung sowie Ort, Datum und Uhrzeit der Erfassung – unverzüglich gelöscht werden. Art. 38 Abs. 3 PAG-Bay macht hiervon eine Ausnahme, wenn ein Trefferfall vorliegt und die weitere Speicherung der Daten im Einzelfall zur Abwehr einer Gefahr oder zu dem Zweck, zu dem die Fahndungsdatei erstellt wurde, erforderlich ist. In diesem Fall gelten die in Art. 38 Abs. 1, 2 PAG-Bay und der Strafprozessordnung normierten allgemeinen Regelungen zur Speicherung, Veränderung und Nutzung von Daten. Die Erstellung eines Bewegungsprofils durch die Verbindung von Einzelerfassungen darf gem. Art. 38 Abs. 3 S. 3 i.V.m. Art. 33 Abs. 2 S. 3 Nr. 2 a) PAG-Bay nur dann erfolgen, wenn eine Person zur polizeilichen Beobachtung, zur gezielten Kontrolle oder zur verdeckten Registrierung ausgeschrieben ist. Ein flächendeckender Einsatz der automatischen Kennzeichenfahndung wird durch Art. 33 Abs. 2 S. 5 PAG-Bay ausgeschlossen.

Im September 2009 hat das Verwaltungsgericht München die Rechtmäßigkeit der bayerischen Regelung zur automatischen Kennzeichenfahndung bestätigt, eine Berufung zum Bayerischen Verwaltungsgerichtshof jedoch ausdrücklich zugelassen.[90] Der Kläger hat angekündigt, diese Möglichkeit wahrzunehmen und Berufung gegen das Urteil einzulegen.[91]

---

[90] VG München, AZ M 7 K 08.3052 vom 23.09.2009; Nürnberger Zeitung Online, 24.09.2009, siehe: http://www.nz-online.de/artikel.asp?art=1091782&kat=30&man=40 (15.03.2011).

[91] Focus Online, 30.10.2009, siehe: http://www.focus.de/auto/news/recht-kennzeichen-scanning-mitunter-rechtmaessig_aid_449610.html (15.03.2011).

*4.4 Hamburg*

Eine knappe, inhaltlich sehr allgemein gehaltene Regelung zur automatischen Kennzeichenfahndung enthält § 8 Abs. 6 HbgPolEDVG. Danach darf die Polizei „bei Kontrollen im öffentlichen Verkehrsraum nach diesem Gesetz und anderen Gesetzen personenbezogene Daten durch den Einsatz technischer Mittel zur elektronischen Erkennung von Kraftfahrzeugkennzeichen zum Zwecke des automatischen Abgleichs mit dem Fahndungsbestand erheben. Daten, die im Fahndungsbestand nicht enthalten sind, sind unverzüglich zu löschen."

Allerdings wird die automatische Kennzeichenfahndung in Hamburg seit dem Urteil des Bundesverfassungsgerichts vom 11. März 2008 nicht mehr praktiziert.[92] Die Anwendung des § 8 Abs. 6 HbgPolEDVG wurde vorübergehend ausgesetzt, eine Änderung der Norm ist geplant.[93]

*4.5 Hessen*

Als eines der ersten Bundesländer hatte Hessen im Jahr 2005 eine spezielle Ermächtigungsgrundlage zur automatischen Kennzeichenfahndung geschaffen. Der einschlägige § 14 Abs. 5 HSOG lautete wie folgt: „Die Polizeibehörden können auf öffentlichen Straßen und Plätzen Daten von Kraftfahrzeugkennzeichen zum Zwecke des Abgleichs mit dem Fahndungsbestand automatisiert erheben. Daten, die im Fahndungsbestand nicht enthalten sind, sind unverzüglich zu löschen." Am 11. März 2008 erklärte das Bundesverfassungsgericht diese Regelung jedoch – wie auch die entsprechende Norm des Landes Schleswig-Holstein – für verfassungswidrig und daher nichtig.[94]

Im Rahmen einer umfassenden Reform des HSOG wurde mit Wirkung vom 23.12.2009 ein neuer § 14a HSOG geschaffen, welcher eine verfassungskonforme Regelung für den Einsatz von automatischen Kennzeichenlesegeräten bereitstellen soll.[95] Danach kann die Polizei „zur Abwehr einer Gefahr oder zur vorbeugenden Bekämpfung von Straftaten durch den Einsatz technischer Mittel automatisch Bilder von Fahrzeugen aufzeichnen und deren Kennzeichen erfassen", sofern die Voraussetzungen einer Identitätsfeststellung nach § 18 Abs. 1, 2 Nr. 1, 3 - 6 HSOG gegeben sind. Die Maßnahme darf demnach an besonders gefährlichen oder gefährdeten Orten sowie an Orten, an denen sich Straftäter verbergen oder Personen der Prostitution nachgehen, durchgeführt werden. Ferner ist sie an bestimmten Kontrollstellen sowie zur Bekämpfung der grenzüberschreitenden Kriminalität an Einrichtungen des internationalen

---

92 ADAC: Kennzeichenscanning – Umsetzung der Vorgaben des Bundesverfassungsgerichts (2009), siehe: http://www.adac.de/_mm/pdf/ga_ks_05_expertise0409_adac_gutachten_kurzfassung_49296.pdf (15.03.2011).

93 Koalitionsvereinbarung vom 17. April 2008, siehe: http://www.cduhamburg.de/27002/Uploaded/2008_koalitionsvertrag.pdf (15.03.2011).

94 Siehe BVerfG, 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008.

95 Siehe GVBl. Hessen 2009, Teil I, Nr. 21, S. 635 f.

Verkehrs und an Straßen, die nach Lageerkenntnissen der Polizei für den grenzüberschreitenden Verkehr von erheblicher Bedeutung sind, zulässig.

Die erfassten Kennzeichen „können automatisch mit dem Fahndungsbestand der Sachfahndungsdateien des beim BKA nach den Vorschriften des BKAG und des beim hessischen LKA nach den Vorschriften dieses Gesetzes geführten polizeilichen Informationssystems" einschließlich der Ausschreibungen im SIS abgeglichen werden. In § 14a Abs. 2 S. 3 HSOG wird der Fahndungsbestand weiter eingegrenzt und konkretisiert. Gem. § 14a Abs. 2 S. 4 HSOG muss der Abgleich sofort nach der Datenerhebung erfolgen. Ein Abgleich mit Kennzeichenfragmenten ist nicht zulässig. Zudem dürfen anhand der erlangten Daten gem. § 14a Abs. 2 S. 5 HSOG keine Bewegungsbilder erstellt werden. Gemäß Art. 14a Abs. 1 S. 3 HSOG darf die automatische Kennzeichenfahndung nicht flächendeckend und nur in bestimmten Fällen dauerhaft oder längerfristig durchgeführt werden.

Ist das erfasste Kennzeichen nicht im Fahndungsbestand, müssen die erhobenen Daten nach § 14a Abs. 3 HSOG sofort automatisiert gelöscht werden. Eine Protokollierung der Datenerhebung und des Datenabgleichs ist in diesen Fällen nicht zulässig. Die Durchführung der Maßnahme muss jedoch nach § 14a Abs. 1 S. 4 HSOG in für Kontrollzwecke geeigneter Weise dokumentiert werden.

Wird im Rahmen des Kennzeichenabgleichs ein Treffer erzielt, kann das entsprechende Kennzeichen samt Trefferbild und Angaben zu Tag, Ort und Uhrzeit der Erfassung sowie der Fahrtrichtung des betroffenen Fahrzeugs gespeichert werden. Das weitere Vorgehen richtet sich sodann nach Art. 14a Abs. 4 S. 2 - 4 HSOG.

### *4.6 Mecklenburg-Vorpommern*

Eine umfassende Regelung zur automatischen Kennzeichenfahndung enthält auch das SOG M-V. Gemäß § 43a Abs. 1 i.V.m. §§ 27a, 29, 32, 33 Abs. 1 Nr. 1 SOG M-V ist die Maßnahme immer dann zulässig, wenn die Voraussetzungen für eine polizeiliche Anhalte- und Sichtkontrolle, eine Identitätsfeststellung, für den Einsatz technischer Mittel zur Bildüberwachung, zur Bild- und zur Tonaufnahme oder für eine Observation gegeben sind. Sie darf also insbesondere zur vorbeugenden Bekämpfung grenzüberschreitender Kriminalität im Grenzgebiet bis zu einer Tiefe von 30 km sowie der in § 49 SOG M-V genannten schweren Straftaten durchgeführt werden. Des Weiteren ist die automatische Kennzeichenfahndung zulässig, sofern sie zur Abwehr bevorstehender Gefahren, zum Schutz von Personen oder Objekten an besonders gefährdeten Orten i.S.d. § 29 Abs. 1 S. 1 Nr. 2, 3 SOG M-V und zur Verhinderung geplanter Straftaten im Zusammenhang mit öffentlichen Veranstaltungen oder Ansammlungen erforderlich ist.

Grundsätzlich muss die Maßnahme in Mecklenburg-Vorpommern offen durchgeführt werden. Nur wenn dies die Erfüllung polizeilicher oder ordnungsbehördlicher Aufgaben erheblich gefährden würde oder wenn eine verdeckte Durchführung im Interesse des Betroffenen liegt, kann die Maßnahme gem. § 43a Abs. 1 S. 2 i.V.m. § 26 Abs. 2 SOG M-V auch verdeckt erfolgen.

Die erlangten Daten dürfen zunächst gem. § 43a Abs. 1 S. 1 SOG M-V „mit dem Fahndungsbestand" abgeglichen werden. Darüber hinaus ermächtigt § 43a Abs. 2 SOG M-V zu einem Abgleich mit „anderen polizeilichen Dateien", sofern diese „zur Abwehr von im Einzelfall oder im Hinblick auf bestimmte Ereignisse allgemein bestehende Gefahren errichtet wurden und der Abgleich zur Abwehr einer solchen Gefahr erforderlich ist". Ergibt der Abgleich keinen Treffer, sind die erlangten Kennzeichendaten gem. § 43a Abs. 3 SOG M-V unverzüglich zu löschen.

*4.7 Niedersachsen*

In Niedersachsen ist die Durchführung einer automatischen Kennzeichenfahndung gem. § 32 Abs. 5 S. 1 NdsSOG zur Abwehr einer Gefahr für die öffentliche Sicherheit, zur Verhütung der in § 14 Abs. 1 NdsSOG genannten Straftaten und „zur Verhütung von Straftaten von erheblicher Bedeutung mit internationalem Bezug" zulässig. Des Weiteren darf sie an „gefährlichen Orten" i.S.d. § 13 Abs. 1 Nr. 2 NdsSOG zur Verhütung bestimmter Straftaten, sowie in unmittelbarer Nähe der in § 13 Abs. 1 Nr. 3 NdsSOG beschriebenen gefährdeten Objekte durchgeführt werden.

Neben dem Kennzeichen werden gem. § 32 Abs. 3 S. 2 NdsSOG Datum, Ort und Uhrzeit erfasst und ein Bild von dem jeweiligen Fahrzeug angefertigt. Allerdings muss es gem. § 32 Abs. 3 S. 2 NdsSOG technisch ausgeschlossen sein, dass die Insassen des Fahrzeuges zu sehen sind oder sichtbar gemacht werden können. Die erfassten Kennzeichen müssen gem. § 32 Abs. 5 S. 3, 4 NdsSOG sofort automatisiert mit der Fahndungsliste abgeglichen und im Nichttrefferfall gelöscht werden. Die Fahndungsliste enthält Dateien, welche der Suche nach Personen oder Sachen dienen oder zur Kontrollmeldung ausgeschriebene Kennzeichen beinhalten.

Auch in Niedersachsen muss die automatische Kennzeichenfahndung grundsätzlich offen durchgeführt werden, in verdeckter Form ist sie gem. § 32 Abs. 5 S. 6 NdsSOG nur zulässig, wenn andernfalls der Zweck der Maßnahme gefährdet würde.

Schließlich weist § 32 Abs. 2 S. 5 NdsSOG noch darauf hin, dass die im Trefferfall gespeicherten Daten nicht zu einem Bewegungsbild verbunden werden dürfen. Etwas anderes gilt nur, wenn eine Ausschreibung zur Kontrollmeldung vorliegt.

Gegen diese niedersächsische Regelung zur automatischen Kennzeichenfahndung wurde im Mai 2008 ebenfalls Verfassungsbeschwerde eingelegt.[96]

*4.8 Rheinland-Pfalz*

Gem. § 27 Abs. 5 S. 1 RhPfPOG kann die Polizei des Landes Rheinland-Pfalz bei allen „Kontrollen im öffentlichen Verkehrsraum nach diesem Gesetz und andere Gesetzen" eine

---

[96] Siehe http://www.daten-speicherung.de/data/Klageschrift_Kfz-Massenscanning_Nds_2008-05-26_anon.pdf (15.03.2011).

automatische Kennzeichenfahndung durchführen. Dabei werden die erlangten Kennzeichendaten „mit dem Fahndungsbestand" abgeglichen. Welche Daten der „Fahndungsbestand" umfassen darf, wird nicht näher umschrieben.

In verdeckter Form ist die Maßnahme gem. § 27 Abs. 5 S. 2 RhPfPOG nur zulässig, wenn andernfalls der Zweck der Maßnahme gefährdet würde. Die unvermeidbare Betroffenheit Dritter steht der Zulässigkeit dieser Maßnahmen gem. § 27 Abs. 6 S. 1 RhPfPOG nicht entgegen. Gem. § 27 Abs. 6 S. 2 RhPfPOG sind die durch die Maßnahme erlangten Daten „unverzüglich, spätestens nach zwei Monaten zu löschen oder zu vernichten, soweit diese nicht zur Verfolgung von Straftaten oder Ordnungswidrigkeiten von erheblicher Bedeutung, zur Gefahrenabwehr, insbesondere zur vorbeugenden Bekämpfung von Straftaten, oder zur Behebung einer bestehenden Beweisnot, erforderlich sind."

Besonders hervorzuheben ist § 27 Abs. 7 RhPfPOG: Dieser verlangt, dass auf eine offene Datenerhebung, die länger als 48 Stunden am Stück durchgeführt wird, „in geeigneter Weise hingewiesen" wird, „soweit dadurch nicht der Zweck der Maßnahme gefährdet wird". Eine derartige Hinweispflicht bei Durchführung einer automatischen Kennzeichenfahndung ist in keinem anderen Landesgesetz vorgesehen.

### *4.9 Saarland*

Die Vollzugspolizei des Saarlandes darf die automatische Kennzeichenfahndung gem. § 27 Abs. 3 SPolG „zur Abwehr einer Gefahr bei Kontrollen auf öffentlichen Straßen und Plätzen" einsetzen. Die Maßnahme muss grundsätzlich offen erfolgen; nur wenn dadurch der Zweck der Maßnahme vereitelt würde, ist eine verdeckte Durchführung zulässig. Gem. § 27 Abs. 3 S. 1 SPolG dürfen die erlangten Daten ganz allgemein „mit dem Fahndungsbestand" abgeglichen werden. Zudem ist gem. § 27 Abs. 3 S. 3 SPolG ein Abgleich „mit anderen polizeilichen Dateien" immer dann zulässig, wenn „die Dateien zur Abwehr von im Einzelfall oder im Hinblick auf bestimmte Ereignisse bestehenden Gefahren errichtet wurden und der Abgleich zur Abwehr einer solchen Gefahr erforderlich ist". Eine Verpflichtung zur sofortigen Löschung der erhobenen Daten im Nichttrefferfall ergibt sich aus § 27 Abs. 5 S. 2 SPolG.

### *4.10 Schleswig-Holstein*

Von April 2007 bis April 2009 enthielt auch § 184 LVwG-SH in seinem Absatz 5 eine Regelung zur automatischen Kennzeichenfahndung. Diese lautete wie folgt: „Die Polizei kann bei Kontrollen im öffentlichen Verkehrsraum nach diesem Gesetz und anderen Gesetzen personenbezogene Daten durch den offenen Einsatz technischer Mittel zur elektronischen Erkennung von Kraftfahrzeugkennzeichen zum Zwecke des automatisierten Abgleichs mit dem Fahndungsbestand erheben. Eine verdeckte Datenerhebung ist nur zulässig, wenn durch die offene Datenerhebung der Zweck der Maßnahme gefährdet würde. Sofern auf das abgefragte Kennzeichen keine Fahndungsnotierung besteht, sind die gewonnenen Daten unverzüglich zu löschen. Besteht zu dem abgefragten Kennzeichen eine Fahndungsnotierung, gilt Absatz 4

Satz 3 bis 5 entsprechend. Der flächendeckende stationäre Einsatz technischer Mittel nach den Sätzen 1 und 2 ist nicht zulässig."

Am 11. März 2008 erklärte das Bundesverfassungsgericht diese Norm, gemeinsam mit der hessischen Regelung zur automatischen Kennzeichenfahndung[97], für verfassungswidrig und daher nichtig.[98] Daraufhin wurde § 184 LVwG-SH mit Wirkung vom 27. April 2009 aufgehoben. Die Einführung einer neuen Regelung zur automatischen Kennzeichenfahndung ist derzeit nicht geplant.[99]

### *4.11 Thüringen*

In Thüringen ist eine automatische Kennzeichenfahndung gem. § 33 Abs. 7 i.V.m. § 14 Abs. 1 Nr. 2 - 4 PAG-Th an „gefährlichen Orten" i.S.d. § 14 Abs. 1 Nr. 2, 3 PAG-Th unter den dort genannten Voraussetzungen sowie an einer Kontrollstelle zur präventiven Abwehr von Straftaten i.S.d. § 100a StPO und § 27 VersG zulässig. Dabei werden das Kfz-Kennzeichen, Ort, Datum, Uhrzeit und Fahrtrichtung der vorbeifahrenden Fahrzeuge automatisiert erhoben und zur Datenübertragung zwischengespeichert. Diese Daten dürfen ausschließlich für einen sofortigen Datenabgleich, welcher der Verhütung oder Unterbindung von Straftaten oder der Eigentumssicherung dient, genutzt werden.

Als Besonderheit ist hervorzuheben, dass eine automatische Kennzeichenfahndung nach § 33 Abs. 7 S. 1 PAG-Th nur dann zulässig ist, „wenn eine Anhaltemöglichkeit der Person zur Identitätsfeststellung gewährleistet ist". Des Weiteren gehört Thüringen zu den wenigen Bundesländern, die – wie auch Baden-Württemberg, Bayern und Hessen – eine flächendeckende Durchführung dieser Maßnahme ausdrücklich verbieten.

### *4.12 Andere Bundesländer*

Die Länder Nordrhein-Westfahlen, Sachsen und Sachsen-Anhalt haben die automatische Kennzeichenfahndung bislang nicht speziell geregelt. Auch in Berlin existiert derzeit keine spezielle Regelung zur automatischen Kennzeichenfahndung, die Maßnahme wird dort aber gleichwohl durchgeführt.[100]

In Bremen[101] und Schleswig-Holstein[102] gab es zwar zeitweilig eine Regelung, diese wurden aber wieder aufgehoben bzw. ausgesetzt.

---

[97] Siehe oben 4.5.

[98] Siehe Fn.86.

[99] ADAC, siehe Fn.92.

[100] ADAC, siehe Fn. 92.

[101] Ehem. § 29 Abs. 6 BremPolG: in Kraft vom 17.03.2006 bis 23.07.2008.

[102] Ehem. § 184 Abs. 5 LVwG: in Kraft vom 27.04.2007 bis 27.04.2009.

### *4.13 Zusammenfassung*

Die zehn derzeit bestehenden landesrechtlichen Regelungen zur automatischen Kennzeichenfahndung weisen im Hinblick auf Inhalt und Umfang eine zum Teil erhebliche Varianz auf. Gemeinsam ist allen Regelungen, dass die Maßnahme – obwohl sie sehr kontrovers diskutiert wird – keiner richterlichen Anordnung bedarf.

Auffallend ist auch, dass diverse Bundesländer einen allgemeinen Abgleich der erfassten Kennzeichen „mit dem Fahndungsbestand"[103] vorsehen, ohne diesen genauer zu definieren bzw. zu begrenzen. Welche Kennzeichen in die zum Abgleich erstellte Fahndungsliste aufgenommen werden, geht aus diesen Vorschriften nicht hervor. In seinem Urteil zur automatischen Kennzeichenfahndung vom 11. März 2008 hat das Bundesverfassungsgericht in derartigen Formulierungen einen Verstoß gegen das verfassungsrechtliche Gebot der Zweckbindung gesehen und sie mangels Normenklarheit und -bestimmtheit als verfassungswidrig eingestuft.[104] Allerdings hat das Bundesverfassungsgericht auch darauf hingewiesen, dass ein weit gefasster Verwendungszweck nicht per se verfassungswidrig sein muss. Vielmehr könne der Verwendungszweck durchaus weit gefasst werden, sofern er mit engen Eingriffsvoraussetzungen kombiniert wird. Als Beispiel hierfür hebt das Bundesverfassungsgericht die brandenburgische Regelung zur automatischen Kennzeichenfahndung positiv hervor.[105] Wegen ihrer besonders detaillierten Beschreibung des zum Abgleich eingesetzten Fahndungsbestandes sind darüber hinaus auch die Regelungen der Länder Baden-Württemberg, Bayern und Hessen hervorzuheben.

Des Weiteren hat das Bundesverfassungsgericht darauf hingewiesen, dass ein flächendeckender Einsatz der automatischen Kennzeichenfahndung nicht zulässig sei.[106] Ausdrücklich geregelt ist dies nur in den Gesetzestexten der Länder Baden-Württemberg, Bayern, Hessen und Thüringen.

Während die Hälfte der Bundesländer keine Angabe dazu macht, welche Daten bei der Erfassung der Kraftfahrzeuge erhoben werden, wird dies von einzelnen Bundesländern[107] genau festgelegt. Die Länder Baden-Württemberg, Hessen und Niedersachsen machen sogar Angaben darüber, was auf dem Bild erkennbar sein darf: Während die Insassen des Fahrzeuges in Baden-Württemberg erkennbar sein dürfen, sofern dies unvermeidbar ist, muss dies nach dem niedersächsischen SOG technisch ausgeschlossen sein.

Zudem treffen nur Baden-Württemberg und Hessen eine explizite Regelung zur Dauer der Maßnahme. Indirekt impliziert auch das rheinland-pfälzische Polizei- und Ordnungsbehördengesetz, dass die Maßnahme jedenfalls länger als 48 Stunden am Stück andauern darf.

---

103 So z.B. Hessen, Mecklenburg-Vorpommern und Rheinland-Pfalz.

104 Siehe BVerfG, 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008, Ls. 3 und Abs. 93 ff.

105 Siehe BVerfG, 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008, Abs. 183.

106 Siehe BVerfG, 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008, Ls. 4 und Abs. 172.

107 Baden-Württemberg, Bayern, Hessen, Niedersachsen, Thüringen.

Auch nachdem das Bundesverfassungsgericht Stellung zur automatischen Kennzeichenfahndung bezogen hat, dauert die Diskussion um Reichweite und Grenzen dieser Maßnahme an. Dazu trägt auch der Umstand bei, dass weitere Klagen in diesem Bereich anhängig sind. So hat der in erster Instanz beim Verwaltungsgericht München mit seinen Einwänden gegen die bayerische Regelung unterlegene Kläger Berufung angekündigt. Gegen die Regelungen in Baden-Württemberg und Niedersachsen wurden weitere Verfassungsbeschwerden eingelegt.

# Übersicht 1: Verkehrsdatenabfrage

| Bundesland | Baden-Württemberg<br>§ 23a V PolG | Bayern<br>§ 34b II Nr.1, 2, III PAG | Berlin | Brandenburg<br>§ 33b VI 2 PolG |
|---|---|---|---|---|
| **Voraussetzungen** | Abs.5 i.V.m. Abs.1:<br>- unmittelbar bevorstehende Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leben, Gesundheit oder Freiheit einer Person<br>- über Personen, wenn Tatsachen die Annahme rechtfertigen, dass sie schwerwiegende Straftaten i.S.d. Abs.2 begehen werden oder daran beteiligt sein werden | Abs.2 Nr.1, 2 i.V.m. § 34a I 1, III 1 PAG:<br>- dringende Gefahr für Bestand oder Sicherheit des Bundes oder eines Landes oder für Leben, Gesundheit oder Freiheit einer Person od. für eine Sache, soweit eine gemeine Gefahr besteht<br>- Besonderheit: nur für Zielsuchlauf wird vorausgesetzt, dass die Erforschung des Sachverhalts sonst aussichtslos oder wesentl. erschwert wäre (Abs.2 S.2) | - | Abs. 6 S. 2 i.V.m. Abs. 1, 2 i.V.m. § 33a I PolG:<br>- dringende Gefahr für Leib, Leben oder Freiheit einer Person<br>- wenn tatsächliche Anhaltspunkte für die geplante Begehung einer Katalogtat des § 33a I PolG vorliegen<br>- betrifft Person des potentiellen Straftäters sowie seiner Kontakt- oder Begleitpersonen i.S.d. § 33a II 3-5 |
| **Richtervorbehalt** | + (Abs.3) | + (§ 34 c I i.V.m. § 34 IV 1, 2 PAG) | | - |
| Durchbrechung bei Gefahr im Verzug | +<br>Anordnung durch Regierungspräsidenten, Leiter des LKA, eines Polizeipräsidiums oder einer Polizeidirektion möglich;<br>teilw. kann Anordnungsbefugnis auf besonders beauftragte Beamte des höheren Dienstes übertragen werden (Abs.3 S.7 i.V.m. § 23 III S.8 i.V.m. § 22 VI PolG) | +<br>Anordnung durch Leiter eines Präsidiums der Landespolizei oder des LKA; Übertragung auf Beamte des höheren Polizeivollzugsdienstes möglich | | |
| **Wenn Dritte betroffen** | wenn unvermeidbar (Abs.1 S.4) | - | | - |
| **Mitwirkungspflicht d.Telekommunikationsunternehmen** | + (Abs.5) | + | | + |

# Übersicht 1: Verkehrsdatenabfrage (2)

| **Bundesland** | **Bremen** | **Hamburg**<br>§ 10b IV PolEDVG | **Hessen**<br>§ 15a I, II HSOG | **Mecklenburg-Vorpommern**<br>§ 34a V, VI SOG |
|---|---|---|---|---|
| **Voraussetzungen** | - | Abs.4 i.V.m. Abs.1 i.V.m. § 10a PolEDVG:<br>- unmittelbar bevorstehende Gefahr für Leib, Leben oder Freiheit einer Person<br>- Besonderheit: nur für Zielsuchlauf wird vorausgesetzt, dass die Erforschung des Sachverhalts auf andere Weise aussichtslos wäre (§ 10b II PolEDVG) | - gegenwärtige Gefahr für Leib, Leben oder Freiheit einer Person | Abs.5 i.V.m. Abs.1 Nr.1, Abs.2 Nr.2:<br>- bevorstehende Gefahr für Leib, Leben oder Freiheit einer Person oder den Bestand oder die Sicherheit des Bundes oder eines Landes |
| **Richtervorbehalt** | | + (§10c I PolEDVG) | + (Abs.5) | Nur bei besonderem Vertrauensverhältnis (Abs.4 i.V.m.§ 34 III1) |
| Durchbrechung bei Gefahr im Verzug | | +<br>Anordnung durch den Polizeipräsidenten | + | +<br>Anordnung durch Behördenleiter |
| **Wenn Dritte betroffen** | | wenn unvermeidbar (§ 10a I 2PolEDVG) | - | wenn unvermeidbar →unverz. Löschung (Abs.1 S.3, Abs.8 S.4) |
| **Mitwirkungspflicht d.Telekommunikationsunternehmen** | | + (Abs.4) | + (Abs.1) | + (Abs.6) |

# Übersicht 1: Verkehrsdatenabfrage (3)

| **Bundesland** | **Niedersachsen**<br>§ 33a VII SOG | **Nordrhein-Westfalen** | **Rheinland-Pfalz**<br>§ 31 POG | **Saarland**<br>§ 28b PolG |
|---|---|---|---|---|
| **Voraussetzungen** | Abs.2 S.1 Nr.2 i.V.m. Abs.1:<br>- Gefahr für Leib, Leben oder Freiheit einer Person | - | Abs.6 i.V.m. Abs.1, 2 Nr.2:<br>- gegenwärtige Gefahr für Leib oder Leben einer Person | Abs.2 i.V.m. Abs.1:<br>- gegenwärtige Gefahr für Leib, Leben oder Freiheit einer Person<br>- zur vorbeugenden Bekämpfung der in § 100c StPO genannten Straftaten, wenn Tatsachen die Annahme begründen, dass bestimmte Personen diese Straftaten begehen werden |
| **Richtervorbehalt** | + (Abs.4) | | + (Abs.5) | teilw. (Abs.5) |
| Durchbrechung bei Gefahr im Verzug | +<br>Anordnung durch Behördenleiter der Polizei (Abs.5) | | +<br>Anordnung durch die Behördenleitung oder einen von ihr besonders beauftragten Beamten des höheren Dienstes | +<br>Behördenleitung od. besonders beauftragter Beamter d. höheren PVollzD |
| **Wenn Dritte betroffen** | wenn unvermeidbar (Abs.2 S.3) | | wenn unvermeidbar (Abs.2 S.1) | wenn unvermeidbar (Abs.1 S.4) |
| **Mitwirkungspflicht d.Telekommunikationsunternehmen** | + (Abs.7) | | + (Abs.6) | + (Abs.2) |

# Übersicht 1: Verkehrsdatenabfrage (4)

| Bundesland | Sachsen | Sachsen-Anhalt | Schleswig-Holstein §185a IV LVwG | Thüringen § 34a I S.1 Nr.3, III PAG |
|---|---|---|---|---|
| **Voraussetzungen** | - | - | Abs.4 i.V.m. Abs.2 Nr.2 i.V.m. Abs.1:<br>- Gefahr für Leib, Leben oder Freiheit einer Person | Abs.1, 3:<br>- dringende 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<br>- wenn Tatsachen die Annahme rechtfertigen, dass eine Person eine Straftat i.S.d. § 31 V PAG plant oder an der Planung oder der Tat beteiligt ist |
| **Richtervorbehalt** | | | + (§ 186 I 1 LVwG) | + (Abs.5) |
| Durchbrechung bei Gefahr im Verzug | | | +<br>Anordnung durch Leiter des Polizeiamtes, des LKA oder einer Polizeidirektion; Übertragung auf besonders beauftragte des Polizeivollzugsdienstes möglich<br>(§ 186 I 2-5) | +<br>Anordnung durch den Leiter den Polizeibehörde oder bei Verhinderung durch dessen Stell-vertreter (Abs.5 S.2) |
| **Wenn Dritte betroffen** | | | wenn unvermeidbar (§ 185a III 4 i.V.m. § 185 IV LVwG) | wenn unvermeidbar (Abs.3 S.3) |
| **Mitwirkungspflicht d.Telekommunikationsunternehmen** | | | + (Abs.4) | + (Abs.1 S.1 Nr.3) |

# Übersicht 2: Standortbestimmung

| Bundesland | Baden-Württemberg<br>§ 23a VI 1 Nr.1PolG | Bayern<br>§ 34a II S.1 Nr.2, III S.1 Nr.2 PAG | Berlin<br>§ 25a II ASOG | Brandenburg<br>§ 33b III Nr. 2 PolG |
|---|---|---|---|---|
| **Voraussetzungen** | Abs.6 i.V.m. Abs.1:<br>- unmittelbar bevorstehende Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leben, Gesundheit oder Freiheit einer Person<br>- über Personen wenn Tatsachen die Annahme rechtfertigen, dass sie schwerwiegende Straftaten i.S.d. Abs. 2 begehen werden oder daran beteiligt sein werden | Abs.2, 3 i.V.m. Abs.1:<br>- dringende Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leben, Gesundheit oder Freiheit einer Person oder für eine Sache, soweit eine gemeine Gefahr besteht | Abs.2 i.V.m. Abs.1:<br>- gegenwärtige Gefahr für Leib oder Leben einer Person<br>- nur Ortung des Handys der gefährdeten Person zulässig | Abs.3 i.V.m. Abs.1, 2 i.V.m. § 33a I PolG:<br>- dringende Gefahr für Leib, Leben oder Freiheit einer Person<br>- wenn tatsächliche Anhaltspunkte für die geplante Begehung einer Katalogtat des § 33a I PolG vorliegen<br>- betrifft Person des potentiellen Straftäters sowie seiner Kontakt- oder Begleitpersonen i.S.d. § 33a II 3-5 |
| **Richtervorbehalt** | -<br>Anordnung durch Regierungspräsidenten, Leiter des LKA, eines Polizeipräsidiums oder einer Polizeidirektion möglich;<br>teilw. kann Anordnungsbefugnis auf besonders beauftragte Beamte des höheren Dienstes übertragen werden (Abs.6 S.3 i.V.m. § 22 VI PolG) | +<br>(§ 34 c I i.V.m. § 34 IV 1 PAG) | -<br>Polizei und Feuerwehr zuständig | + (Abs.5) |
| Durchbrechung bei Gefahr im Verzug | | § 33 V: Leiter eines Landespolizeipräsidiums od. des LKA; Übertragung mögl. | | +<br>Behördenleiter |
| **Wenn Dritte betroffen** | wenn unvermeidbar (Abs.6 S.2) | wenn unvermeidbar → unverz.Löschung (Abs.2 S.2, 3) | wenn unvermeidbar → unverzügliche Löschung (Abs.3) | wenn unvermeidbar → unverzügliche Löschung (Abs.4) |
| **Mitwirkungspflicht d.Telekommunikationsunternehmen** | - | +<br>(§34b II 1Nr.3 PAG) | +<br>(Abs.1) | +<br>(Abs.6 S.1) |

## Übersicht 2: Standortbestimmung (2)

| **Bundesland** | **Bremen**<br>§ 33 I PolG | **Hamburg**<br>§ 10b III 1 Nr. 2 PolEDVG | **Hessen**<br>§ 15a III HSOG | **Mecklenburg-Vorpommern**<br>§ 34a SOG |
|---|---|---|---|---|
| **Voraussetzungen** | Abs.1 S.1 i.V.m. § 32 I 1 PolG:<br>- gegenwärtige Gefahr für Leib, Leben oder Freiheit einer Person<br>- Beobachtung von Personen, bei denen Tatsachen die Annahme recht-fertigen, dass sie Straftaten von erheblicher Bedeutung begehen werden.<br>- Kontaktpersonen letzterer | - unmittelbar bevorstehende Gefahr für Leib, Leben oder Freiheit einer Person | - gegenwärtige Gefahr für Leib, Leben oder Freiheit einer Person | Abs.2 Nr. 3 i.V.m. Abs. 1:<br>- bevorstehende Gefahr für Leib, Leben oder Freiheit einer Person oder den Bestand oder die Sicherheit des Bundes oder eines Landes |
| **Richtervorbehalt** | -<br>„Der Polizeivollzugsdienst darf ..." | + (§10c I PolEDVG) | + (Abs.5) | Nur bei besonderem Vertrauensverhältnis (Abs.4 i.V.m. § 34 III1) |
| Durchbrechung bei Gefahr im Verzug | | +<br>Anordnung durch Polizeipräsidenten | + | +<br>Anordnung durch Behördenleiter |
| **Wenn Dritte betroffen** | wenn unvermeidbar (Abs.1 S.2) | wenn unvermeidbar (Abs.3 S.4) | - | wenn unvermeidbar →unverz. Löschung (Abs.1 S.3, Abs.8 S.4) |
| **Mitwirkungspflicht d.Telekommunikations-unternehmen** | - | + (Abs.4 S.1 Nr.3) | + (Abs.1) | + (Abs.6) |

# Übersicht 2: Standortbestimmung (3)

| Bundesland | Niedersachsen<br>§ 33a SOG | Nordrhein-Westfalen | Rheinland-Pfalz<br>§ 31 POG | Saarland<br>§ 28b I PolG |
|---|---|---|---|---|
| **Voraussetzungen** | Abs.2 S.1 Nr.3 i.V.m. Abs.1:<br>- Gefahr für Leib, Leben oder Freiheit einer Person | - | Abs.2 Nr.3 i.V.m. Abs.1:<br>- gegenwärtige Gefahr für Leib oder Leben einer Person | - gegenwärtige Gefahr für Leib, Leben oder Freiheit einer Person<br>- zur vorbeugenden Bekämpfung der in § 100c StPO genannten Straftaten, wenn Tatsachen die Annahme begründen, dass bestimmte Personen diese Straftaten begehen werden |
| **Richtervorbehalt** | + (Abs.4)<br>Ausnahme: dient die Maßnahme ausschließlich der Ermittlung des Aufenthaltsortes der gefährdeten Person, trifft die Polizei die Anordnung | | + (Abs.5) | - in Fällen des Abs.1 S.1 Nr.1 (Gefahr für Leib, Leben oder Freiheit einer Person)<br>+ in Fällen des Abs.1 S.1 Nr.2 (vorbeugende Bekämpfung der in § 100c StPO genannten Straftaten): Anordnung durch Behördenleitung; Übertragung auf besonders Beauftragten mögl. (Abs.5, 6) |
| Durchbrechung bei Gefahr im Verzug | +<br>Anordnung durch Polizei (Abs.5) | | +; Behördenleitung od. besonders beauftragter Beamter d. höheren Dienstes | +; Behördenleitung od. besonders beauftragter Beamter d. höheren PVollzD |
| **Wenn Dritte betroffen** | wenn unvermeidbar (Abs.2 S.3) | | wenn unvermeidbar (Abs.2 S.1) | wenn unvermeidbar (Abs.1 S.4) |
| **Mitwirkungspflicht d.Telekommunikationsunternehmen** | + (Abs.7) | | + (Abs.6) | + (Abs.2) |

## Übersicht 2: Standortbestimmung (4)

| Bundesland | Sachsen | Sachsen-Anhalt | Schleswig-Holstein §185a LVwG | Thüringen § 34a II S.1 Nr.3, III PAG |
|---|---|---|---|---|
| **Voraussetzungen** | - | - | Abs.2 Nr.3 i.V.m. Abs.1:<br>- Gefahr für Leib, Leben oder Freiheit einer Person | Abs.3:<br>- dringende 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<br>- wenn Tatsachen die Annahme rechtfertigen, dass eine Person eine Straftat i.S.d. § 31 V PAG plant oder an der Planung oder der Tat beteiligt ist |
| **Richtervorbehalt** | | | + (§ 186 I 1 LVwG) | + (Abs.5) |
| Durchbrechung bei Gefahr im Verzug | | | +; Leiter d. Polizeiamtes, des LKA oder einer Polizeidirektion; Übertragung auf PVD mögl. | +<br>Leiter der Polizeibehörde; bei Verhinderung dessen Stellvertreter |
| **Wenn Dritte betroffen** | | | wenn unvermeidbar (§ 185a III 4 i.V.m. § 185 IV LVwG) | wenn unvermeidbar (Abs.3 S.3) |
| **Mitwirkungspflicht d.Telekommunikationsunternehmen** | | | + (Abs.4) | - |

## Übersicht 3: automatische Kennzeichenfahndung

| | **Baden-Württemberg** § 22a PolG | **Bayern** Art. 33 II 2-5, Art. 38 III, Art. 46 II 4 PAG | **Berlin** | **Brandenburg** § 36a PolG |
|---|---|---|---|---|
| **Voraussetzungen** | detaillierte Regelung in Abs.1 i.V.m. § 26 I PolG: zur Abwehr einer Gefahr oder zur vorbeugenden Bekämpfung von Straftaten bei Kon-trollen nach § 26 I PolG (Personenfeststellung) | detaillierte Regelung in Art. 33 II i.V.m. Art. 13 I PAG (Identitäts-feststellung) und Art.30 III 2 PAG (Erfüllung polizeilicher Aufgaben auf andere Weise gefährdet oder erheblich erschwert od. überwiegendes Interesse des Betroffenen) | - | detaillierte Regelung in Abs.1 i.V.m. §§ 12 I, 36 I, Ia PolG: - gegenwärtige Gefahr für Leib oder Leben einer Person - gegenwärtige Gefahr bei Vorliegen der Voraussetzungen für eine Identitätsfeststellung (§ 12 I PolG) - polizeilich ausgeschriebenes Fahrzeug (§ 36 I, Ia) |
| **offen / verdeckt** | verdeckt | verdeckt | | k.A. |
| **Anordnungsbefugnis** | Polizeivollzugsdienst | „die Polizei" | | „die Polizei" |
| **Bildaufzeichnung von Insassen** | wenn unvermeidbar (Abs.1 S.2) | k.A. | | k.A. |
| **Flächendeckend** | nicht zulässig (Abs.1 S.3 Nr.1) | nicht zulässig (Art. 33 II 5) | | k.A. |
| **Längerfristig / Dauerhaft** | teilweise ausgeschlossen (Abs.1 S.3 Nr.2, 4) | k.A. | | k.A. |
| **Fahndungsbestand** | Sachfahndungsdateien der beim BKA nach dem BKAG geführten Informationssysteme inkl. Ausschreibungen im SIS; Beschränkung auf bestimmte Fahrzeuge (Abs.2) | polizeilichen Fahndungsbeständen i.S.d. Art. 33 II 3, 4 | | „zur Abwehr der Gefahr nach Abs. 1 gespeicherten polizeilichen Daten" (Abs.2 S.1) |
| **Löschung im Nichttrefferfall** | unverzüglich und automatisch (Abs.3 S.1) | unverzüglich (Art. 38 III 1) | | unverzüglich (Abs.2 S.3) |
| **Gespeicherte Daten im Trefferfall** | Kennzeichen, Bild, Ort, Datum, Uhrzeit, Fahrtrichtung | Kennzeichen, Ort, Datum, Uhrzeit, Fahrtrichtung | | k.A. |
| **Hinweise** | Neu eingeführt m.W.v. 22.11.2008; Verfassungsbeschwerde wurde im November 2009 eingereicht | Neufassung m.W.v. 01.01.2008; VG München bestätigte die Rechtmäßigkeit der bayerischen Regelung (23.09.2009) | wird trotz Fehlen einer spez. RGL durchgeführt und auf § 25 I Nr.2 ASOG (Datenerhebung durch Einsatz techn. Mittel) gestützt | |

# Übersicht 3: automatische Kennzeichenfahndung (2)

| | Bremen | Hamburg<br>§ 8 VI PolEDVG | Hessen<br>§ 14a HSOG | Mecklenburg-Vorpommern<br>§ 43a SOG |
|---|---|---|---|---|
| **Voraussetzungen** | - | „bei Kontrollen im öffentlichen Verkehrsraum nach diesem Gesetz und anderen Gesetzen" | detaillierte Regelung in Abs.1 i.V.m. § 18 HSOG: zur Abwehr einer Gefahr oder zur vorbeugenden Bekämpfung von Straftaten | detaillierte Regelung in Abs.1 i.V.m. § 27a SOG (Polizeiliche Anhalte- und Sichtkontrollen), § 29 SOG (Identitätsfeststellung), § 32 SOG (Einsatz techn. Mittel zur Bildüberwachung sowie zur Bild- und Tonaufzeichnung) und § 33 I Nr.1 SOG (Observation) |
| **offen / verdeckt** | | k.A. | k.A. | grds. offen; zusätzl. Voraussetz., wenn verdeckt (Abs.1 S.2) |
| **Anordnungsbefugnis** | | „die Polizei" | „die Polizeibehörden" | „die Polizei" |
| **Bildaufzeichnung von Insassen** | | k.A. | wenn unvermeidbar (Abs.1 S.2) | k.A. |
| **Flächendeckend** | | k.A. | nicht zulässig (Abs.1 S.3 Nr.1) | k.A. |
| **Längerfristig / Dauerhaft** | | k.A. | teilweise ausgeschlossen (Abs.1 S.3 Nr.2, 4) | k.A. |
| **Fahndungsbestand** | | nicht näher konkretisiert | Sachfahndungsdateien der beim BKA und beim hess. LKA geführten Informationssysteme inkl. Ausschreibun-gen im SIS; Beschränkung auf bestimmte Fahrzeuge (Abs.2) | nicht näher konkretisiert (Abs.1 S.1); sofern zur Gefahrenabwehr erforderlich ist auch ein Abgleich mit anderen (genauer beschrie-benen) polizeilichen Dateien (Abs.2) |
| **Löschung im Nichttrefferfall** | | unverzüglich (Abs.6 S.2) | sofort automatisiert (Abs. 3 S.1) | unverzüglich (Abs.3) |
| **Gespeicherte Daten im Trefferfall** | | k.A. | Kennzeichen, Bild, Ort, Datum, Uhrzeit, Fahrtrichtung | k.A. |
| **Hinweise** | ehem. § 29 VI PolG: am 17.03.2006 in Kraft getreten; m.W.v. 23.07.2008 aufgehoben | laut ADAC-Gutachten in der Praxis ausgesetzt | *ehem. § 14 V HSOG wurde vom BVerfG am 11.03.2008 für verfassungswidrig u. nichtig erklärt | |

# Übersicht 3: automatische Kennzeichenfahndung (3)

| | **Niedersachsen**<br>§ 32 V SOG | **Nordrhein-Westfalen** | **Rheinland-Pfalz**<br>§ 27 V POG | **Saarland**<br>§ 27 III, V 2 SPolG |
|---|---|---|---|---|
| **Voraussetzungen** | detaillierte Regelung in Abs.5 S.1 i.V.m. § 13 Abs. 1 SOG (Identitätsfeststellung) und § 14 Abs. 1 S. 1 SOG (Kontrollstellen) | - | Abs.5 S.1:<br>- „bei Kontrollen im öffentlichen Verkehrsraum nach diesem Gesetz und anderen Gesetzen" | Abs.3 S.1:<br>- „zur Abwehr einer Gefahr bei Kontrollen auf öffentlichen Straßen und Plätzen" |
| **offen / verdeckt** | grds. offen; verdeckt nur bei Zweckgefährdung (Abs.5 S.6) | | grds. offen; verdeckt nur bei Zweckgefährdung (Abs.5 S.2) | grds. offen; verdeckt nur bei Zweckgefährdung (Abs.3 S.2) |
| **Anordnungsbefugnis** | „die Polizei" | | „die Polizei" | Vollzugspolizei |
| **Bildaufzeichnung von Insassen** | nicht zulässig (Abs.5 S.2) | | k.A. | k.A. |
| **Flächendeckend** | k.A. | | k.A. | k.A. |
| **Längerfristig / Dauerhaft** | k.A. | | k.A. | k.A. |
| **Fahndungsbestand** | Abgleich „mit vorhandenen Dateien..., die der Suche nach Personen oder Sachen dienen oder in denen Kennzeichen (...) zur Kontrollmeldung ausgeschrieben sind" (Abs.5 S.3) | | nicht näher konkretisiert | Abgleich „mit dem Fahndungsbestand" (Abs.3 S.1);<br>mit anderen polizeilichen Dateien nur unter zusätzl. Voraussetzungen (Abs.3 S.3) |
| **Löschung im Nichttrefferfall** | sofort (Abs.5 S.4) | | unverzügl., spätest. nach 2 Mo. mit Ausnahme (Abs.6 S.2) | sofort (Abs.5 S.2) |
| **Gespeicherte Daten im Trefferfall** | Kennzeichen, Bild, Ort, Datum, Uhrzeit | | k.A. | k.A. |
| **Hinweise** | Neufassung m.W.v. 24.01.2009;<br>Verfassungsbeschwerde wurde im Mai 2008 beim BVerfG eingereicht | | Hinweis, wenn offen, länger als 48 Std. und keine Zweckgefährdung; laut ADAC-Gutachten in der Praxis ausgesetzt | |

# Übersicht 3: automatische Kennzeichenfahndung (4)

| | Sachsen | Sachsen-Anhalt | Schleswig-Holstein | Thüringen<br>§ 33 VII PAG |
|---|---|---|---|---|
| **Voraussetzungen** | - | - | - | detaillierte Regelung in Abs.7 S.1 i.V.m. § 14 I Nr.2 - 4 PAG (Identitätsfeststellung); neben den Voraussetzungen des § 14 I Nr. 2 - 4 PAG muss eine Anhaltemöglichkeit der Person zur Identitätsfeststellung gewährleistet sein |
| **offen / verdeckt** | | | | k.A. |
| **Anordnungsbefugnis** | | | | „die Polizei" |
| **Bildaufzeichnung von Insassen** | | | | k.A. |
| **Flächendeckend** | | | | nicht zulässig (Abs.7 S.2) |
| **Längerfristig / Dauerhaft** | | | | k.A. |
| **Fahndungsbestand** | | | | „für einen sofortigen Datenabgleich zur Verhütung oder Unterbindung von Straftaten oder zur Eigentumssicherung" |
| **Löschung im Nichttrefferfall** | | | | Zwischenspeich. zur Datenübertragung zulässig (Abs.7 S.1) |
| **Gespeicherte Daten im Trefferfall** | | | | Kennzeichen, Bild, Ort, Datum, Uhrzeit, Fahrtrichtung |
| **Hinweise** | | | ehem.§ 184 V LVwG am 27.04.2007 in Kraft getreten; am 11.03. 2008 vom BVerfG für verfassungswidrig & nichtig erklärt; m.W.v. 27.04. 2009 aufgehoben | Neu eingeführt m.W.v. 30.07.2008 |

# Teil C: Internationaler Rechtsvergleich

## 1. England & Wales

Sämtliche Maßnahmen, welche mit der Abfrage von Verkehrsdaten in Zusammenhang stehen oder eine Form der verdeckten Überwachung darstellen, fallen in England und Wales in den Anwendungsbereich des Gesetzes zur Regelung von Ermittlungsbefugnissen (*Regulation of Investigatory Powers Act 2000*, im Folgenden: RIPA). Sein Hauptzweck besteht darin, eine menschenrechtskonforme Anwendung von Ermittlungsbefugnissen sicherzustellen.[108] Da die Standortermittlung mit der Verkehrsdatenabfrage in Zusammenhang steht, fällt auch diese in den Anwendungsbereich des RIPA. Bei der automatischen Kennzeichenfahndung ist danach zu unterscheiden, ob sie in offener oder in verdeckter Form durchgeführt wird.

### *1.1 Verkehrsdatenabfrage und Ortung von Mobiltelefonen*

Nach § 22 Abs. 2 i.V.m. § 21 Abs. 4, 6 RIPA sind die Verkehrsdatenabfrage und die Standortermittlung zulässig zum Schutz der inneren Sicherheit, zur Prävention und Aufklärung von Kriminalität, zur Aufrechterhaltung der öffentlichen Sicherheit und Ordnung, im Interesse des wirtschaftlichen Wohlergehens des Vereinigten Königreiches, zum Schutz der Volksgesundheit, für die Einziehung von Steuergeldern und Gebühren, im Notfall zum Schutz von Leib und Leben sowie für sonstige Zwecke, die der Innenminister in einem speziellen Erlass festgelegt hat. Bei diesem Erlass handelt es sich um den sog. *Regulation of Investigatory Powers (Communication Data) Order 2003*[109], der durch den *Regulation of Investigatory Powers (Communication Data) (Additional Functions and Amendment) Order 2006*[110] ergänzt wird. In diesen beiden Erlassen wird ferner geregelt, wer für die Anordnung einer Verkehrsdatenabfrage bzw. einer Standortermittlung zuständig ist. Die dort nach Funktion und Dienstgrad genau benannten Personen gehören allesamt einer der in § 25 Abs. 1, 2 RIPA genannten Behörde an. Darüber hinaus hat das Innenministerium gem. § 71 Abs. 1, 2, 4 RIPA einen *Code of Practice*[111] erlassen, der eine verbindliche Leitlinie für die Durchführung einer Verkehrsdatenabfrage oder Standortermittlung darstellt. Die Mitwirkungspflicht der Telekommunikationsunternehmen ergibt sich aus § 22 Abs. 4, 5 RIPA.

---

[108] Explanatory Notes to the Regulation of Investigatory Power Act – Summary and Background; siehe: http://www.opsi.gov.uk/acts/acts2000/en/ukpgaen_20000023_en_1 (15.03.2011).

[109] Statutory Instrument 2003 No. 3172.

[110] Statutory Instrument 2006 No. 1878.

[111] Acquisition and Disclosure of Communications Data Code of Practice; siehe: http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/code-of-practice-acquisition?view=Binary (15.03.2011).

*1.2 Automatische Kennzeichenfahndung*

Bezüglich des Einsatzes von automatischen Kennzeichenlesesystemen wird in England und Wales nicht zwischen der automatischen Kennzeichenfahndung und der automatischen Kennzeichenerfassung unterschieden. An zahlreichen Stellen im Land werden die Kennzeichen aller vorbeifahrenden Fahrzeuge erfasst und mit Angaben zu Ort, Datum und Zeit der Erfassung an eine spezielle Behörde, das *National ANPR Data Centre* (NADC), übermittelt. Dort werden die erhobenen Daten überprüft, bearbeitet und bis zu fünf Jahren gespeichert.[112] Täglich übermitteln die Polizeikräfte des Landes ca. 10 Millionen Datensätze an das NADC, im Jahr beläuft sich die Summe auf ca. 3.650 Millionen Datensätze.[113] Aus welchem Grund eine automatische Kennzeichenfahndung oder -erfassung durchgeführt wurde und ob die Maßnahme offen oder verdeckt erfolgte, wird den gespeicherten Kennzeichen nicht zugeordnet. Daher kann nicht in Erfahrung gebracht werden, wie oft die Maßnahme zwecks Gefahrenabwehr oder Kriminalprävention durchgeführt wird und wie viele der gespeicherten Daten aus einer präventiv-polizeilichen Erhebung stammen.[114]

Die Zulässigkeit einer verdeckt durchgeführten automatischen Kennzeichenfahndung richtet sich nach den Vorschriften des RIPA. Wird die Maßnahme hingegen offen durchgeführt, muss sie nach Angaben des britischen Innenministeriums, des *Home Office*, nicht den im RIPA niedergelegten Anforderungen genügen.[115]

Gem. §§ 26, 27 Abs. 1, 48 Abs. 2 RIPA ist die automatische Kennzeichenfahndung als verdeckte Maßnahme zur gezielten Suche nach einer bestimmten Person zu jedem beliebigen Zweck zulässig, sofern eine entsprechende Genehmigung vorliegt. Diese soll jedoch nur erteilt werden, wenn die Maßnahme im Interesse und zum Schutz der inneren Sicherheit, zur Prävention und Aufklärung von Kriminalität, zur Aufrechterhaltung der öffentlichen Sicherheit und Ordnung, im Interesse des wirtschaftlichen Wohlergehens des Vereinigten Königreiches, zum Schutz der Volksgesundheit oder für die Einziehung diverser Steuergelder und Gebühren erforderlich und verhältnismäßig ist. Zur Erteilung dieser Genehmigung sind gem. § 30 Abs. 1, 4 RIPA nur dazu speziell ermächtigte Personen befugt, welche einer der in Anhang 1 des RIPA aufgelisteten Behörden angehören und in einem Erlass des Innenministers[116] nach Position und Dienstgrad genau bezeichnet werden. Die Genehmigung muss

---

112 http://www.independent.co.uk/news/science/surveillance-uk-why-this-revolution-is-only-the-start-520396.html; http://www.boingboing.net/2009/11/21/traffic-cameras-used.html; National Policing Improvement Agency: http://www.npia.police.uk/en/10505.htm (15.03.2011).

113 Angaben der National Policing Improvement Agency.

114 Angaben der National Policing Improvement Agency.

115 Beachte aber Art. 1.4 Covert Surveillance Code of Practice: „Although, the provisions of the 2000 Act or of this code of practice do not normally cover the use of overt CCTV surveillance systems, since members of the public are aware that such systems are in use, there may be occasions when public authorities use overt CCTV systems for the purposes of a specific investigation or operation. In such cases, authorisation for intrusive or directed surveillance may be necessary."

116 Regulations of Investigatory Powers (Prescription of Offices, Ranks and Positions) Order 2000, Statutory Instrument 2000 No. 2417.

gem. § 33 Abs. 1 RIPA stets von einem Mitglied derselben Truppe beantragt und außer bei Gefahr im Verzug schriftlich erteilt werden. Sie gilt gem. § 43 Abs. 3 RIPA 12 Monate, eine mündlich erteilte Genehmigung hingegen nur 72 Stunden. Für jede Genehmigung besteht gem. § 43 Abs. 4, 6, 7 RIPA die Möglichkeit einer Verlängerung. Auch zur verdeckten Überwachung samt automatischer Kennzeichenfahndung hat das Innenministerium gem. §§ 71, 72 RIPA einen sog. *Code of Practice* erlassen.[117] Dieser soll gewährleisten, dass die nach dem RIPA zulässigen Maßnahmen auch in rechtmäßiger Weise durchgeführt werden. Einen weiteren Leitfaden mit demselben Ziel speziell für die automatische Kennzeichenfahndung hat die Nationale Behörde zur Verbesserung der Polizeitätigkeit (*National Policing Improvement Agency*, NPIA) im Auftrag der Gesellschaft der Polizeipräsidenten (*Association of Chief Police Officers*, ACPO) zusammengestellt.[118]

## 2. Finnland

Das finnische Recht unterscheidet – wie auch das deutsche Recht – zwischen der Durchführung von polizeilichen Maßnahmen zu repressiven Zwecken und solchen zwecks Gefahrenabwehr und Kriminalprävention. Während erstere im Gesetz über Zwangsmaßnahmen (*Pakkokeinò-laki*)[119] geregelt sind, richten sich präventiv-polizeiliche Maßnahmen nach dem Polizeigesetz (*Poliisilaki*, im Folgenden: PolL)[120]. Zu beachten ist, dass beide Gesetze derzeit überarbeitet werden und sich daher in nächster Zeit Änderungen ergeben können.

### *2.1 Verkehrsdatenabfrage und Ortung von Mobiltelefonen*

In Kapitel 3 PolL befinden sich Regelungen zur Informationsgewinnung. Bei der Verkehrsdatenabfrage und der Standortermittlung handelt es sich um Maßnahmen, die unter den Begriff der Telefonüberwachung im Sinne des PolL 28 Nr. 6 § fallen. Sie sind gem. PolL 31b § zur Verfolgung der dort genannten Verbrechen zulässig und müssen außer bei Gefahr im Verzug gem. PolL 32b - 33 § von einem Richter angeordnet werden. Darüber hinaus darf gem. PolL 31f § das Mobiltelefon einer sich in Gefahr befindenden Person geortet werden.

### *2.2 Automatische Kennzeichenfahndung*

Hinsichtlich der automatischen Kennzeichenfahndung gibt es im finnischen Polizeirecht keine spezielle Ermächtigungsgrundlage. Insbesondere wird die Maßnahme nicht als eine solche zur Informationsgewinnung, sondern als „normale Überwachungstätigkeit" angesehen, die in den Anwendungsbereich der polizeilichen Generalklausel (PolL 1 §) fällt. Allerdings wird die automatische Kennzeichenfahndung in Finnland noch nicht praktiziert. Derzeit wird jedoch

---

117 Covert Surveillance Code of Practice; siehe: http://www.torbay.gov.uk/covert-cop.pdf (15.03.2011).

118 Practice Advice on the Management and Use of Automatic Number Plate Recognition 2009; siehe: http://www.acpo.police.uk/documents/crime/2009/200907CRIANP01.pdf (15.03.2011).

119 450/1987.

120 492/1995.

eine ähnliche Technik getestet, bei der Kameras, die ebenfalls Kennzeichen lesen können, aus Polizeiautos heraus zum Einsatz kommen. Diese Maßnahme wird auf die Regelungen zur technischen Überwachung und zur technischen Observation i.S.d. PolL 28 Nr. 1, Nr. 3, 29, 31 § gestützt.

## 3. Frankreich

In Frankreich ist die Zuständigkeit für den Bereich der Gefahrenabwehr und der Kriminalprävention zwischen nationalen und lokalen Behörden aufgeteilt: während der Staat Sicherheit gewährleisten soll, liegt die Zuständigkeit im Bereich der Kriminalprävention bei den lokalen Hoheitsträgern. Insbesondere bestimmt der Bürgermeister in seinem Gebiet die Richtlinien der Politik zur Kriminalprävention und koordiniert deren Umsetzung. Im Übrigen fehlt es aber weitgehend an einer klaren Abgrenzung und Zuweisung der Zuständigkeiten.[121]

Mit Erlass des Gesetzes bezüglich des Kampfes gegen den Terrorismus (*Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité aux contrôles frontaliers*; im Folgenden: LLT)[122] wurden im Jahr 2006 die Vorschriften diverser Gesetze überarbeitet und verschiedene präventiv-polizeiliche Maßnahmen neu geregelt. Der Conseil Constitutionnel, das französische Verfassungsgericht, hatte das Gesetz vor seinem Erlass überprüft und im Wesentlichen für verfassungsgemäß erklärt.[123]

### *3.1 Verkehrsdatenabfrage und Ortung von Mobiltelefonen*

Mit Art. 6 Abs. 1 LLT wurde in das Gesetz bezüglich der Post und elektronischer Kommunikation (*Code des postes et des communications électroniques*; im Folgenden: CPCE) ein neuer Art. 34-1-1 eingeführt. Danach können speziell dazu berufene Mitglieder der Polizei und der Gendarmerie von Telekommunikationsanbietern die Herausgabe diverser gespeicherter Daten verlangen. Nach Abs. 2 des Art. 34-1-1 CPCE unterliegen auch die Verkehrsdaten und die für eine Handyortung erforderlichen Daten der Auskunftspflicht. Derartige Anfragen müssen gem. Art. 34-1-1 Abs. 4 CPCE vorweg vom Innenministerium genehmigt werden. Einem Richtervorbehalt unterliegen die Verkehrsdatenabfrage und die Standortermittlung seit Erlass des LLT nicht mehr.[124]

Nach dem durch Art. 6 Abs. 3 LLT geänderten Art. 27 des Gesetzes über die Geheimhaltung der Kommunikation (*Loi relative au secret des correspondances émises par la voie des communications électroniques*)[125] ist für die Maßnahmen nach Art. 34-1-1 CPCE ein nationaler

---

121 European Crime Prevention Network: „Crime Prevention in France", siehe: http://eucpn.org/strat docs/eucpn_crime_prevention_strategy_France.pdf (15.03.2011).

122 Loi n°2006-64.

123 Décision n° 2005-532 DC vom 19.01.2006.

124 *Albrecht/Grafe/Kilchling*: Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungen nach §§ 100g, 100h StPO, S. 67, Fn. 347.

125 Loi n° 91-646.

Kontrollausschuss für Überwachungsmaßnahmen und Sicherheit, die *Commission nationale de contrôle des interceptions de sécurité*, zuständig.

*3.2 Automatische Kennzeichenfahndung*

Die Zulässigkeit der automatischen Kennzeichenfahndung richtet sich nach dem durch Art. 8 LLT geänderten Art. 26 des Gesetzes zur Inneren Sicherheit (*Loi pour la sécurité intérieure*; im Folgenden: LSI)[126]. Dieser ermächtigt die Polizei, die Gendarmerie und den Zoll dazu, an allen Orten, an denen es zweckmäßig ist, insbesondere im Bereich von Grenzübergängen, Häfen und Flughäfen sowie auf großen nationalen und internationalen Verkehrsachsen, sowohl stationäre, als auch mobile Einrichtungen zur automatisierten Kontrolle von Kfz-Erkennungsdaten einzusetzen. Darüber hinaus darf die Maßnahme unter anderem zur Vorbeugung von Terroranschlägen, zum Erhalt der öffentlichen Sicherheit sowie bei bestimmten Veranstaltungen und bei großen Versammlungen durchgeführt werden. Dabei dürfen auch die Insassen der betroffenen Kraftfahrzeuge fotografiert werden. Das genaue Verfahren und die weitere Verwendung der Daten werden in Art. 26 Abs. 2 - 5 LSI geregelt.

**4. Österreich**

In Österreich sind gem. § 21 Sicherheitspolizeigesetz (SPG)[127], die Sicherheitsbehörden für die Gefahrenabwehr und die Kriminalprävention zuständig. Sie haben allgemeine Gefahren abzuwehren, gefährlichen Angriffen unverzüglich ein Ende zu setzen und Gruppierungen zu beobachten, „wenn im Hinblick auf deren bestehende Strukturen und auf zu gewärtigende Entwicklungen in deren Umfeld damit zu rechnen ist, dass es zu mit schwerer Gefahr für die öffentliche Sicherheit verbundener Kriminalität, insbesondere zu weltanschaulich oder religiös motivierter Gewalt, kommt". Die in § 21 SPG verwendeten Begriffe der allgemeinen Gefahr und des gefährlichen Angriffs werden in § 16 Abs. 1 - 3 SPG legaldefiniert.

Darüber hinaus sieht § 19 SPG eine „erste allgemeine Hilfeleistungspflicht" der Sicherheitsbehörden vor, welche diese ungeachtet der Zuständigkeit einer anderen Behörde zur Abwehr einer gegenwärtigen oder unmittelbar bevorstehenden Gefahr für Leben, Gesundheit, Freiheit oder Eigentum verpflichtet.

Zur Erfüllung dieser Aufgaben statten die §§ 28 ff. SPG die Sicherheitsbehörden mit diversen polizeilichen Befugnissen aus. Darunter befinden sich auch Regelungen zur Verkehrsdatenabfrage, der Handyortung und der automatischen Kennzeichenfahndung. Der Datenschutzbeauftragte muss gem. § 91c Abs. 1 S. 3 SPG über jede dieser Maßnahme informiert werden. Zudem muss ihm gem. § 91d Abs. 2 SPG jederzeit Gelegenheit gegeben werden, die Durchführung dieser Maßnahmen sowie die Löschung der erhobenen Daten zu überprüfen.

---

126 Loi n° 2003-239.

127 Bundesgesetz über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei, [österr.] BGBl. Nr. 566/1991, zuletzt geändert durch Bundesgesetz vom 30.12.2009, BGBl. I Nr. 133/2009.

*4.1 Verkehrsdatenabfrage und Ortung von Mobiltelefonen*

Gem. § 53 Abs. 3a SPG dürfen die Sicherheitsbehörden von den Telekommunikationsunternehmen diverse Daten abfragen, sofern bestimmte Tatsachen die Annahme einer konkreten Gefahrensituation rechtfertigen und die Sicherheitsbehörden die Verkehrsdaten „als wesentliche Voraussetzung für die Erfüllung der ihnen nach diesem Bundesgesetz übertragenen Aufgaben benötigen". Hinsichtlich eines bestimmten Telefonanschlusses beschränkt sich diese Befugnis gem. § 53 Abs. 3a S. 1 Nr. 1 SPG jedoch auf den Namen des Anschlussinhabers, dessen Anschrift und die entsprechende Teilnehmernummer. Nur zur Erfüllung einer ersten allgemeinen Hilfeleistungspflicht i.S.d. § 19 SPG und zur Abwehr gefährlicher Angriffe i.S.d. § 15 Abs. 2, 3 SPG kann „durch Bezeichnung eines möglichst genauen Zeitraumes und der passiven Teilnehmernummer" auf ein von diesem Anschluss geführtes Gespräch Bezug genommen werden. Gem. § 53a Abs. 3a S. 3 SPG müssen die Telekommunikationsunternehmen die Auskunft unverzüglich und kostenlos erteilen.

Sofern eine gegenwärtige Gefahr für Leben oder Gesundheit eines Menschen besteht, ermächtigt § 53 Abs. 3b SPG die Sicherheitsbehörden ferner zur Abfrage der Standortdaten und der IMSI-Nummer desjenigen Mobiltelefons, welches von der gefährdeten Person mitgeführt wird. In diesen Fällen werden den Telekommunikationsunternehmen die angefallenen Kosten gem. § 53 Abs. 3b S. 3 SPG i.V.m. § 7 Z. 4 der Überwachungskostenverordnung (ÜKVO) erstattet.

Neben einer Verkehrsdatenabfrage ermöglicht § 53 Abs. 3b SPG unter denselben Voraussetzungen auch die Ortung desjenigen Mobiltelefons, welches eine gefährdete Person bei sich führt.

Zu beachten ist, dass in Österreich derzeit an der Umsetzung der Richtlinie zur Vorratsdatenspeicherung[128] gearbeitet wird. In diesem Rahmen wurde am 22. Februar 2011 vom Ministerrat ein Entwurf zur Novellierung des Telekommunikationsgesetzes beschlossen. Daneben müssen auch das SPG und die österreichische Strafprozessordnung geändert und – insbesondere zur Regelung technischer Details – verschiedene ministerielle Verordnungen erlassen werden.[129] Diese sollen spätestens im Mai dieses Jahres beschlossen werden, sodass die Vorratsdatenspeicherung zum 1.1.2012 in Kraft treten kann.[130] Abzuwarten bleibt, inwiefern sich daraus Veränderungen im Hinblick auf die Verkehrsdatenabfrage und die Ortung von Mobiltelefonen ergeben werden.

---

[128] Richtlinie 2006/24/EG.

[129] *Hack*: So funktioniert die Vorratsdatenspeicherung, http://help.orf.at/stories/1676648/ (15.03.2011).

[130] *Kremer*: Österreich: Vorratsdatenspeicherung soll 2012 in Kraft treten, http://www.gulli.com/news/-sterreich-vorratsdatenspeicherung-soll-2012-in-kraft-treten-2011-02-25 (15.03.2011); siehe auch http://www.gulli.com/news/-sterreich-einigt-sich-in-sachen-vorratsdatenspeicherung-2011-02-21 (15.03.2011).

*4.2 Automatische Kennzeichenfahndung*

Die automatische Kennzeichenfahndung ist in § 54 Abs. 4b SPG geregelt. Zu präventivpolizeilichen Zwecken ist sie gem. § 54 Abs. 4b i.V.m. § 24 Abs. 1 Nr. 3, 4 SPG nur zulässig, wenn eine Person „auf Grund einer psychischen Behinderung hilflos ist oder Leben oder Gesundheit anderer ernstlich und erheblich gefährdet" oder wenn dadurch der Aufenthaltsort eines Minderjährigen auf Ersuchen der Eltern ermittelt werden soll. Die Maßnahme ist gem. § 54 Abs. 4b S. 2 SPG auf maximal einen Monat zu beschränken. Im Nichttrefferfall dürfen die erhobenen Daten gem. § 59 Abs. 2 S. 3 SPG nicht protokolliert werden. Liegt hingegen ein Trefferfall vor, müssen die erlangten Daten gem. § 54 Abs. 4b S. 3 SPG gelöscht werden, sobald sie für die konkrete Fahndung nicht mehr benötigt werden.

## 5. Polen

Das polnische Recht kennt, entsprechend der Situation in zahlreichen anderen europäischen Rechtsordnungen, keine der deutschen Rechtslage vergleichbare strikte Trennung zwischen der präventiven und repressiven Zweckbestimmung polizeilicher Maßnahmen. Die Durchführung operativer Maßnahmen der Polizei findet ihre Rechtsgrundlagen übereinstimmend im polnischen Polizeigesetz[131], unabhängig davon, ob diese Maßnahmen präventiven oder repressiven Zielen dienen. Gemäß Art. 14 Abs. 1 des polnischen Polizeigesetzes dürfen operative Maßnahmen grundsätzlich zur Erforschung, Verhinderung und Entdeckung von Straftaten und Ordnungswidrigkeiten durchgeführt werden.[132]

*5.1 Verkehrsdatenabfrage und Ortung von Mobiltelefonen*

Das polnische Polizeigesetz enthält eine explizite Regelung zum Umgang mit Verkehrsdaten, die in Abweichung von der oben genannten generellen Ermächtigungsgrundlage ausdrücklich auf den präventiven Einsatz beschränkt ist. Art. 20c des Gesetzes ermächtigt die Polizei, für Zwecke der Verhinderung und Entdeckung von Straftaten auf Verkehrsdaten zuzugreifen. Neben der Gewinnung der Daten ist ausdrücklich auch deren Verarbeitung, namentlich deren Abgleich erlaubt. Der Begriff der Verkehrsdaten (Telekommunikationsverbindungsdaten) ist in Art. 180c des Telekommunikationsgesetzes[133] definiert: Darunter fallen die Verbindungsdaten im engeren Sinne (Datum, Uhrzeit, Dauer der Verbindung), die Art der Verbindung, bei mobilen Endgeräten der aktuelle Standort (Funkzelle), auch in Echtzeit, sowie die Personenangaben zum Anschlussinhaber.[134] Der Zugriff ist generell erlaubt; Beschränkungen auf

---

131 Ustawa o Policji, Gesetz vom 4.4.1990 (Dz.U. – Gesetzblatt – 2007, Nr. 43, Pos. 277).

132 Einzelheiten hierzu und zu den nachfolgend zitierten Bestimmungen des Polizeigesetzes bei *Kotowski*: Ustawa o Policji. Komentarz. 2. Auflage, Warschau 2008.

133 Prawo telekomunikacyjne, Gesetz vom 16.7.2004 (Dz.U. – Gesetzblatt – 2005, Nr. 108, Pos. 908).

134 Einzelheiten bei *Krasuski*: Prawo telekomunikacyjne. Komentarz. 3. Auflage, Warschau 2009.

bestimmte Straftaten bzw. Rechtsgüter wie auch weitere Anforderungen hinsichtlich Dringlichkeit bzw. Gefahrengrad enthält das Gesetz ausdrücklich nicht.

Anders als in Deutschland unterliegt der polizeiliche Zugriff auf die Verkehrsdaten in Polen keinem Richtervorbehalt; das Gesetz nimmt insoweit eine klare Abstufung zwischen der Auswertung der Verkehrsdaten einerseits und der echten Inhaltsüberwachung vor.[135] Die Erhebung erfolgt in der Regel im Wege eines Auskunftsverlangens an die Diensteanbieter. Dieses kann mündlich, schriftlich oder elektronisch erfolgen.[136] Zur Anforderung berechtigt sind Polizeibeamte, die von einem Hauptkommandanten der Polizei (auf Woiwodschafts- oder nationaler Ebene) schriftlich ermächtigt worden sind. Die Polizei dürfte[137] die benötigten Daten aber auch selbst erheben, was eine eigenständige Durchführung der Ortung ermöglicht. Nach Erledigung der Maßnahme müssen die Daten vernichtet werden. Für den Fall einer möglichen strafrechtlichen Relevanz eines polizeilichen Vorganges müssen sie nach Durchführung der Maßnahme an die Staatsanwaltschaft übermittelt werden.

### *5.2 Automatische Kennzeichenfahndung*

Gemäß Art. 15 Abs. 1 Nr. 5a des polnischen Polizeigesetzes darf die Polizei an öffentlichen Orten technische Geräte einsetzen. Anders als im Kontext des Art. 129 Abs. 2 Pkt. 9 des polnischen Straßenverkehrsgesetzes[138], das auf die Verkehrssicherheit bezogen ist und sich dementsprechend auf Geschwindigkeitskontrollmessungen beschränkt, erlaubt Art. 15 Abs. 1 Nr. 5a des polnischen Polizeigesetzes einen breiteren Einsatz der technischen Mittel. Die Ermächtigung umfasst sowohl die Beobachtung als auch die Aufzeichnung der Vorgänge an öffentlichen Orten, insbesondere den Straßenverkehr.[139] Beide Techniken bzw. Ziele (Verkehrsüberwachung und allgemeine operative Aufgabenerfüllung) können im Übrigen kombiniert werden, sodass im Rahmen einer Radarkontrolle zur Geschwindigkeitskontrolle gleichzeitig auch eine Kennzeichenfahndung zum Einsatz kommen kann.

## 6. Schweden

Bezüglich der im Folgenden dargestellten Rechtslage in Schweden ist zu beachten, dass auch hier diverse Gesetzesänderungen geplant sind und daher mit entsprechenden Neuregelungen gerechnet werden muss.

---

135 Nur im letzteren Fall, beim ‚klassischen' Abhören, ist, neben einigen anderen heimlichen Überwachungsmaßnahmen wie der akustischen Wohnraumüberwachung oder der akustischen Überwachung außerhalb von Wohnungen, eine richterliche Anordnung erforderlich, §§ 19 u. 20 poln. Polizeigesetz.

136 § 20c Abs. 2 Pkt. 1 bis 3 poln. Polizeigesetz.

137 Ob die polnische Polizei auch über die entsprechende Technik verfügt, wird mit Hinweis auf polizeiliche Geheimhaltungsinteressen nicht kommuniziert.

138 Prawo o ruchu drogowym, Gesetz vom 20.6.1997 (Dz.U. – Gesetzblatt – 2007, Nr. 43, Pos. 277). Kommentierung bei *Pawelec*: Prawo o ruchu drogowym. Komentarz. Warschau 2005.

139 Ein sachlicher Bezug zum Straßenverkehr ist nicht unbedingt erforderlich; die Vorschrift dient daher auch als Rechtsgrundlage für die Videoüberwachung.

*6.1 Verkehrsdatenabfrage und Ortung von Mobiltelefonen*

In Schweden wurde die Richtlinie zur Vorratsdatenspeicherung (RL 2006/24/EG) bislang nicht umgesetzt,[140] sodass keine einheitliche Speicherpraxis bei den Telekommunikationsanbietern besteht. Gleichwohl sind diese dazu verpflichtet, der Polizei all diejenigen Daten, die sie bspw. zu Abrechnungszwecken gespeichert haben, unter bestimmten Voraussetzungen zur Verfügung zu stellen. Einzelheiten dazu werden im schwedischen Datenschutzgesetz (*Personuppgifslag*, PUL)[141], dem Telekommunikationsgesetz (*Lag om elektronisk kommunikation*[142], LEK) sowie dem Prozessgesetzbuch (*Rättegångsbalk*[143], RB) geregelt, die sich inhaltlich teilweise überschneiden.

Nach dem RB ist eine Verkehrsdatenabfrage nur dann zulässig, wenn die Maßnahme der Verfolgung und Aufklärung einer Straftat dient. Während die angeforderten Daten früher mit einer Straftat in Verbindung stehen mussten, die im Mindestmaß mit zwei Jahren Freiheitsstrafe bedroht war, darf eine Verkehrsdatenabfrage seit dem 1. Oktober 2004 schon dann durchgeführt werden, wenn Mindeststrafe für die Verbindungstat bei sechs Monaten Freiheitsstrafe liegt. Sofern diese Grenze nicht überschritten wird, dürfen lediglich Bestandsdaten abgefragt werden. Eine Verkehrsdatenabfrage ist dann unzulässig.

Nach dem LEK ist auch eine Verkehrsdatenabfrage zur Erfüllung präventiv-polizeilicher Aufgaben zulässig. Verkehrsdatenabfragen nach dem LEK bedürfen – anders als jene nach dem RB – keiner richterlichen Anordnung und können von der Polizei eigenständig durchgeführt werden.

Welche Daten die Telekommunikationsunternehmen speichern dürfen, wird im Telekommunikationsgesetz genauer geregelt. Dessen 6 kap. 8 § enthält Sonderregelungen bezüglich der Speicherung und Anonymisierung der Daten, sofern diese von Behörden oder Gerichten benötigt werden, „um Streitigkeiten zu lösen". Zu den abfrageberechtigten Behörden gehören u.a. die Polizei, die Finanzpolizei, die Küstenwacht sowie die Zollbehörden.

Bislang besteht keine gesetzliche Regelung zur Kostentragung. In der Praxis werden die bei der Verkehrsdatenabfrage entstandenen Kosten den Telekommunikationsunternehmen aber erstattet.

Die Ortung eines Mobiltelefons ist im Rahmen eines Strafverfahrens nur dann zulässig, wenn dieses auch tatsächlich genutzt, d.h. eine Verbindung aufgebaut wurde. Sofern das Gerät lediglich eingeschaltet war, ist dessen Lokalisierung zu Strafverfolgungszwecken nicht zulässig. In einem Reformgutachten[144] (*Statens offentliga utredningar*, SOU) wurde vorgeschla-

---

[140] Wegen dieses Verstoßes gegen die EU-Richtlinie wurde das Königreich Schweden am 04.02.2010 vom EuGH Verurteilt. Az. C-185/09.

[141] 1998:204.

[142] 2003:389.

[143] 1942:740.

[144] 2009:1.

gen, dass auch die Ortung von Mobiltelefonen im Stand-By-Betrieb zulässig sein sollte. Bislang wurde dieser Vorschlag jedoch nicht umgesetzt.

Mangels Bestehen einer elektronischen Kommunikation ist die Ortung von Mobiltelefonen im LEK nicht vorgesehen. Der Justizkanzler hat darauf hingewiesen, dass die Telekommunikationsunternehmen grundsätzlich auch nicht dazu berechtigt sind, entsprechende Standortdaten herauszugeben, es sei denn, die betroffene Person wird anonymisiert oder sie hat in die Maßnahme eingewilligt. In der Praxis sind wohl Fälle aufgetreten, in denen die Telekommunikationsanbieter den zuständigen Behörden die Standortdaten gleichwohl herausgegeben haben.

### *6.2 Automatische Kennzeichenfahndung*

Eine spezielle Regelung zur automatischen Kennzeichenfahndung gibt es in Schweden bislang nicht. Die entsprechende Technik wird zwar bereits vorgehalten, aufgrund rechtlicher Bedenken bislang aber nicht eingesetzt. Das Reichspolizeiamt prüft derzeit, ob und in welcher Form ein Einsatz technisch möglich und rechtlich zulässig ist.

## 7. Schweiz

In der Schweiz sind die Möglichkeiten einer Informationsbeschaffung zu präventiv-polizeilichen Zwecken eher gering und nur bei unbedingter Notwendigkeit vorgesehen.[145] Daran haben auch die Terroranschläge von New York, London oder Madrid nichts geändert. Selbst ein geplantes Anti-Terror-Gesetzespaket fand nicht die Zustimmung des Parlamentes.[146]

Gleichwohl gibt es diverse Gesetze auf Bundes- und auf kantonaler Ebene, die hoheitliche Maßnahmen zwecks Gefahrenabwehr und Kriminalprävention ermöglichen. Diese sollen im Folgenden dargestellt werden.

Aus den Art. 3, 42 Abs. 1, 43a Abs. 1, 164 der Bundesverfassung der Schweizerischen Eidgenossenschaft (BV)[147] i.V.m. den Verfassungen der Kantone ergibt sich der Grundsatz der kantonalen Gesetzgebungskompetenz. Danach liegt die Gesetzgebungskompetenz für alle Bereiche, welche die BV nicht ausdrücklich dem Bund zuweist, in der Hand der Kantone.[148] Mangels spezieller Zuweisung an den Bund sind daher die Kantone für das Polizeiwesen zuständig.[149] Den Bereich der inneren Sicherheit weist die Bundesverfassung hingegen in Art. 57 und 185 Abs. 2, 3 BV sowohl dem Bund als auch den Kantonen zu. Beide sind dazu

---

145 Auszug aus dem Protokoll des Regierungsrates des Kantons Zürich, Sitzung vom 3. September 2003; vgl. auch http://www.swissinfo.ch/ger/archive.html?siteSect=883&sid=5945203&ty=st (15.03.2011).

146 www.swissinfo.ch/ger/archive.html?siteSect=883&sid=5945203&ty=st (15.03.2011).

147 SR 101.

148 Regierungsrat des Kantons Zürich, siehe Fn. 145.

149 Regierungsrat des Kantons Zürich, siehe Fn. 145.

angehalten, ihre Anstrengungen in diesem Bereich zu koordinieren und abzustimmen. Das kantonale Recht ist als Ergänzung zum jeweils einschlägigen Bundesgesetz anzusehen, es beschreibt dessen Anwendungsbereich genauer und enthält diverse Zuständigkeitsregelungen.

Auf Bundesebene befinden sich Regelungen zur Gefahrenabwehr und Kriminalprävention zunächst im Bundesgesetz über Maßnahmen zur Wahrung der inneren Sicherheit (BWIS)[150]. Dieses weist in § 4 BWIS darauf hin, dass in erster Linie die Kantone für die innere Sicherheit ihres Gebietes verantwortlich sind. Sofern der Bund für die innere Sicherheit verantwortlich ist, leisten die Kantone Amts- und Vollzugshilfe.

Darüber hinaus ist speziell bezüglich der Verkehrsdatenabfrage und der Ortung von Mobiltelefonen das Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF)[151] zu beachten. Die Bundeskompetenz zum Erlass dieses Gesetzes wird auf Art. 92 Abs. 1 BV gestützt, welcher das Post- und Fernmeldewesen dem Bund zuweist.

*7.1 Verkehrsdatenabfrage und Ortung von Mobiltelefonen*

Gem. Art. 1 Abs. 1 Buchst. c) i.V.m. Art. 3 BÜPF darf eine „Überwachung des Fernmeldeverkehrs" als Präventivmaßnahme nur zur Suche nach vermissten Personen, also zur sog. Notsuche, durchgeführt werden. Diese Überwachung muss sich außerdem auf die Teilnehmeridentifikation und die Verkehrsdaten beschränken. Allerdings dürfen gem. Art. 3a Abs. 3 BÜPF auch die Daten unbeteiligter Dritter eingesehen werden. Der Begriff der Verkehrsdaten wird in Art. 2 Buchst. g der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF)[152] definiert und umfasst „alle Informationen, die von der Anbieterin über den ... Fernmeldeverkehr von Teilnehmerinnen und Teilnehmern aufgezeichnet werden, um die Tatsache ... der Kommunikation ... zu belegen". Nach Angaben der Kantonspolizei Zürich fallen hierunter auch die Standortdaten von Mobiltelefonen. Ferner legt Art. 16 VÜPF fest, welche „Überwachungstypen" angeordnet werden können und welche Maßnahmen unter den Begriff der Überwachung i.S.d. Art. 3 BÜPF fallen. Hier werden sowohl die Verkehrsdatenabfrage als auch die Standortermittlung genannt.

Gem. Art. 3 Abs. 2 BÜPF gilt eine Person als vermisst, wenn ihr Aufenthalt unbekannt ist und dringende Anhaltspunkte dafür vorliegen, dass eine schwere Gefährdung für die Gesundheit oder das Leben dieser Person besteht.

Das Verfahren richtet sich gem. Art. 3 Abs. 3 BÜPF nach Art. 274 – 279 der neuen mit Wirkung vom 01.01.2011 in Kraft getretenen eidgenössischen Strafprozessordnung.[153] Aus Art. 274 Abs. 1 StPO i.V.m. Art. 3 Abs. 4 BÜPF ergibt sich, dass eine Verkehrsdatenabfrage und eine Standortbestimmung grundsätzlich von der Staatsanwaltschaft angeordnet werden

---

150 SR 120.

151 SR 780.1.

152 SR 780.11.

153 SR 312.0. Deren Erlass war aufgrund einer Änderung des Art. 123 BV ermöglicht.

kann, die Anordnung jedoch innerhalb von fünf Tagen richterlich bestätigt werden muss. Gemäß Art. 175 StPO muss die Maßnahme unverzüglich beendet werden, sofern deren Voraussetzungen nicht mehr erfüllt sind oder die richterliche Genehmigung verweigert wurde.

Inwiefern die Verkehrsdatenabfrage und die Ortung von Mobiltelefonen zudem auf kantonaler Ebene speziell geregelt sind, soll anhand der exemplarisch ausgewählten Kantone Basel-Stadt, Bern, Freiburg, Nidwalden, Sankt Gallen, Uri und Zürich dargestellt werden.

Während die Kantone Bern, Nidwalden und Sankt Gallen spezielle Regelungen für diese beiden Maßnahmen bereithalten, sind in den Gesetzen der Kantone Basel-Stadt, Freiburg, Uri und Zürich keine entsprechenden Regelungen zu finden. Jedoch sei darauf hingewiesen, dass die Sanität des Kantons **Basel-Stadt** bereits im Jahr 2006 als erste Einsatzzentrale Kontinentaleuropas über eine eigene Software zur Ortung von Mobiltelefonen verfügte.[154]

Der Kanton **Bern** hält in Art. 3 Abs. 2 seines Polizeigesetzes (PolG-BE)[155] eine spezielle Regelung zur Verkehrsdatenabfrage und zur Standortermittlung bereit. Danach ist die Kantonspolizei „für die Anordnung einer Überwachung des Fernmeldeverkehrs (Teilnehmeridentifikation und Verkehrsdaten) außerhalb des Strafverfahrens zuständig, um vermisste Personen zu finden." Hinsichtlich der erforderlichen richterlichen Anordnung verweist Art. 3 Abs. 2 PolG-BS auf die bereits erwähnte bundeseinheitliche StPO[156].

Während das Polizeigesetz des Kantons **Freiburg**[157] wiederum keine spezielle Regelung zur Verkehrsdatenabfrage und der Standortermittlung enthält, hat der Kanton **Nidwalden** im Mai 2009 eine solche in sein Gesetzes über das Polizeiwesen in Nidwalden (PolG-NW)[158] aufgenommen. Nach dem neu geschaffenen Art. 61a PolG-NW sind die Verkehrsdatenabfrage und die Standortermittlung zulässig, sofern die im BÜPF normierten Voraussetzungen vorliegen. Bezüglich des Verfahrens einschließlich der Anordnungskompetenzen verweist Art. 61a Abs. 2 PolG-NW ebenfalls auf die Vorschriften des BÜPF, welches seinerseits auf die Art. 274 – 279 der neuen StPO verweist.

Auch das Polizeigesetz des Kantons **Sankt Gallen** (PolG-SG)[159] hält in Art. 50bis unter Bezugnahme auf das BÜPF eine spezielle Regelung zur Verkehrsdatenabfrage und zur Standortermittlung, welche ebenfalls auf Art. 3a BÜPF verweist. Gem. Art. 50bis PolG-SG ist grundsätzlich der Kommandant der Kantonspolizei für die Anordnung dieser Maßnahmen zuständig. Wird jedoch eine Person „ab der Stadt St. Gallen" vermisst, steht die Anordnungsbefugnis dem Kommandanten der Stadtpolizei St. Gallen zu. Art. 50bis PolG-SG enthält also in erster Linie eine Zuständigkeitsregelung.

---

154 http://tagesschau.sf.tv/nachrichten/archiv/2006/09/25/vermischtes/handy_ortung_bei_sanitaet_notrufen (15.03.2011).

155 SG 510.100.

156 SR 312.0.

157 Gesetz über die Kantonspolizei, RSF 551.1.

158 NW 911.1.

159 SGS 451.1.

Im Kanton **Uri** gab es bis zum 1. Januar 2009 kein einheitliches Polizeigesetz. Vielmehr waren die Aufgaben, die Organisation, die Kompetenzen und die Stellung der Kantonspolizei in vielen unterschiedlichen Erlassen geregelt.[160] Mit dem neuen Polizeigesetz des Kantons Uri (PolG-Uri)[161] sollten diese Schwächen behoben und endlich ein formelles Gesetz geschaffen werden. Im September 2008 sprachen sich 76,8% der Bevölkerung für das neue Polizeigesetz aus,[162] sodass es am 1. Januar 2009 in Kraft treten konnte. Das neue Gesetz lehnt sich in wesentlichen Bereichen an die Gesetze anderer Kantone an,[163] spezielle Regelungen zur Verkehrsdatenabfrage und zur Handyortung enthält es aber nicht.

Noch neuer ist das Polizeigesetz des Kantons **Zürich** (PolG-ZH)[164]: es trat erst am 1. Juli 2009 in Kraft. Im Gegensatz zu anderen kantonalen Polizeigesetzen trennt das neue PolG-ZH streng zwischen dem polizeilichen Handeln im Bereich der Strafverfolgung und jenem zwecks Gefahrenabwehr.[165] Gleichwohl befinden sich auch hier keine speziellen Regelungen zur präventiv-polizeilichen Verkehrsdatenabfrage und der Handyortung.

### *7.2 Automatische Kennzeichenfahndung*

Darzustellen bleibt noch die Rechtslage in der Schweiz zur automatischen Kennzeichenfahndung. Nach Angaben der Kantonspolizei Zürich ist diese Maßnahme Bestandteil der Sachfahndung. Dabei werden die mittels Videokamera erfassten Fahrzeugnummern mit einem automatisierten Polizeifahndungssystem namens „RIPOL" (= frz. *„Recherches informatisées de la police"*) abgeglichen. Bei RIPOL handelt es sich um ein automatisiertes Personen- und Sachfahndungssystem, welches von dem schweizerischen Bundesamt für Polizei „FedPol" in Zusammenarbeit mit den Kantonen betrieben wird. Es soll der Polizei bei der Erfüllung diverser, in Art. 15 Abs. 1 BPI numerisch aufgelisteter Aufgaben dienen. Genannt werden bspw. die Ermittlung des Aufenthalts vermisster Personen, die Ermittlung des Aufenthaltsortes von Kraftfahrzeugführern ohne Versicherungsschutz, die Fahndung nach abhanden gekommenen oder gestohlenen Fahrzeugen und Gegenständen, die Verhinderung von internationaler Kindesentführung und die verdeckte Registrierung oder gezielte Kontrolle von Personen und Fahrzeugen zur Strafverfolgung oder zur Abwehr von Gefahren für die öffentliche Sicherheit. Art. 15 Abs. 1 des Bundesgesetzes über die polizeilichen Informationssysteme des

---

160 Meldung des Regierungsrats vom 27. November 2007, siehe: http://www.ur.ch/de/la/sk/medien mitteilungen-regierungsrat-m657/?m=657&page_no=1&suche_loeschen=1&information_id=3556; Amtsblatt Uri 2008 Nr. 43, S. 16411, siehe: http://www.ur.ch/dateimanager/amtsblatt/2008/amtsblatt_08_43.pdf (15.03.2011).

161 RB 3.8111.

162 Amtsblatt Uri 2008 Nr. 49, S. 1867; siehe: http://www.ur.ch/dateimanager/amtsblatt/2008/amtsblatt_08_49.pdf (15.03.2011).

163 Regierungsrat des Kantons Uri, siehe Fn. 160.

164 LS ZH 550.1.

165 Sicherheitsdirektion des Kantons Zürich: Erläuterungen zum Polizeigesetz, S. 3; siehe: www.ds.zh.ch/internet/ds/de/home/pg.SubContainerList.SubContainer1.ContentContainerList.0006.DownloadFile.pdf (03.12.2009).

Bundes (BPI)[166] regelt den Inhalt, den Zweck und die Zugriffsbefugnisse von RIPOL umfassend. Weitere Einzelheiten hat der Bundesrat in einer gem. Art. 19 BPI erlassenen Verordnung über das automatisierte Polizeifahndungssystem, der sog. RIPOL-Verordnung,[167] festgelegt. Hier ist u.a. geregelt, welche Behörden auf RIPOL zugreifen dürfen (Art. 5 RIPOL-VO), welche Daten bspw. in der Fahrzeugdatenbank (Art. 9, 10 RIPOL-VO) enthalten sind und welche Rechte den Betroffenen zustehen (Art. 17 RIPOL-VO). Gem. Art. 15 Abs. 1 RIPOL-VO werden die Ausschreibungen von Fahrzeugen sofort nach ihrer Eingabe durch die Polizeibehörden der Kantone im RIPOL verarbeitet. Sie können jedoch binnen eines Monats von der ausschreibenden Behörde verändert werden. Nach zwei Monaten wird die eingegebene Fahrzeugfahndung gelöscht, sofern die ausschreibende Behörde sie nicht ausdrücklich aufrechterhält. Wird eine Ausschreibung aufrechterhalten, überprüft FedPol diese und bestätigt sie als definitive Fahndung.

Allerdings wird die automatische Kennzeichenfahndung nach Angaben der Kantonspolizei Zürich derzeit nur zu den in Art. 15 Abs. 1 Buchst. f, g BPI genannten Zwecken durchgeführt, also zur Ermittlung des Aufenthaltes von Kraftfahrzeugführern ohne Versicherungsschutz und zur Fahndung nach abhandengekommenen Fahrzeugen. Zu präventivpolizeilichen Zwecken wird die Maßnahme derzeit also nicht eingesetzt.

## 8. Tschechien

### *8.1 Verkehrsdatenabfrage und Ortung von Mobiltelefonen*

Gemäß Art. 97 § 3 des tschechischen Gesetzes über die elektronische Telekommunikation[168] i.V.m. der Rechtsverordnung Nr. 485/2005 Coll. sind die Telekommunikationsunternehmen dazu verpflichtet, sämtliche Verkehrsdaten einschließlich der Standortdaten sechs Monate lang zu speichern. Diese Daten dürfen von der Polizei zu präventiven Zwecken gem. Art. 71 des tschechischen Polizeigesetzes[169] lediglich im Rahmen der Terrorismusbekämpfung abgefragt werden, sofern eine konkrete Gefahr besteht. Nicht zulässig ist die Abfrage von Verkehrs- und Standortdaten hingegen zur Überwachung einer Person, bei der lediglich der Verdacht besteht, Verbindungen zu terroristischen Netzwerken zu haben, den Terrorismus zu finanzieren oder den Terrorismus auf andere Weise zu fördern. Es handelt sich also um Maßnahmen, die in Tschechien einen sehr begrenzten präventiven Anwendungsbereich haben.

Im Rahmen von Strafverfahren können Verkehrs- und Standortdaten gem. Art. 68 § 2 der tschechischen Strafprozessordnung[170] zur Suche nach Personen sowie gem. Art. 88a der

---

166 SR 361.

167 SR 361.0.

168 Gesetz Nr. 127/2005 Coll., zuletzt geändert durch das Gesetz Nr. 281/2009 Coll.

169 Gesetz Nr. 273/2008 Coll.

170 Gesetz Nr. 141/1961 Coll.

tschechischen Strafprozessordnung im Rahmen einer Telekommunikationsüberwachung abgefragt werden.

*8.2 Automatische Kennzeichenfahndung*

Das tschechische Recht verfügt über keine spezielle Rechtsgrundlage für den Einsatz von automatischen Kennzeichenlesesystemen. Allerdings soll die Maßnahme für den präventiven Bereich vollständig von der Generalklausel in Art. 69 des tschechischen Polizeigesetzes gedeckt sein. Die erhobenen Daten dürfen dann jedoch nur zu präventiven Zwecken und nicht zur Strafverfolgung verwendet werden.

Die automatische Kennzeichenfahndung wird in Tschechien insbesondere an den Grenzübergängen sowie zur Suche nach gestohlenen Kraftfahrzeugen eingesetzt.[171]

## 9. Ungarn

*9.1 Verkehrsdatenabfrage und Ortung von Mobiltelefonen*

Die Abfrage von Verkehrsdaten ist in Ungarn sowohl im Rahmen eines Strafprozesses als auch zu präventiven Zwecken zulässig. Sofern die Maßnahme zu repressiven Zwecken durchgeführt werden soll, richtet sie sich nach Be.71.§ und Be.200.§ der ungarischen Strafprozessordnung[172]. Sie bedarf weder einer staatsanwaltschaftlichen noch einer richterlichen Anordnung. Werden die Verkehrsdaten hingegen zu präventiven Zwecken benötigt, richtet sich ihre Abfrage nach Rtv.63-68.§ des ungarischen Polizeigesetzes[173]. In diesem Fall muss die Maßnahme von der Staatsanwaltschaft genehmigt werden.

Die Ortung von Mobiltelefonen ist demgegenüber nur im Rahmen eines Strafprozesses, nicht aber zu präventiven Zwecken zulässig.

*9.2 Automatische Kennzeichenfahndung*

Die automatische Kennzeichenfahndung wird in Ungarn durch die Polizei in Kooperation mit verschiedenen zivilrechtlichen Organisationen praktiziert. So suchen bspw. die „Internationale Autojägergesellschaft für öffentlichen Nutzen" (*Nemzetközi Autóvadász Közhasznú Egyesület*), das „Zivile Autojägerforum" (*Civil Autóvadász Fórum*) und andere Organisationen mittels einer ungarischen AKLS-Software (*Zsaru-CAR*) nach gestohlenen Kraftfahrzeugen sowie nach Kraftfahrzeugen, die aus anderen, bspw. verwaltungsrechtlichen Gründen auf einer Fahndungsliste stehen. Die dafür erforderlichen Daten werden ihnen über die Webseite der Zentralen Datenregistrierungsbehörde *Központi Adatnyilvántartó Hivata*[174] zur Verfü-

---

171 Siehe www.looksystem.cz.

172 Törvèny a büntetöeljàràsvòl, 19/1998.

173 Törvèny a rendörségröl, 34/1994.

174 http://www.kozpontiadatnyilvantarto.hu/fooldal/ (15.03.2011).

gung gestellt. Diese Webseite ist via Internet mit dem AKLS verbunden und wird ständig aktualisiert.

Zudem setzen auch einzelne lokale Polizeidienststellen, bspw. die Autobahnpolizeien von Dunaújváros, Szigetszentmiklós, Vác, Göd und Nyírbátor, diese Technik ein. Auch die Staatliche Gesellschaft für Autobahnverwaltung (*Magyar Autópályakezelö*) sowie die ungarische Zoll- und Finanzverwaltung (*Vam- és Pénzügyörség*) setzen AKLS ein, unter anderem zur Bekämpfung illegaler Einwanderung. Eine gesetzliche Regelung zum Einsatz von AKLS gibt es in Ungarn bislang jedoch noch nicht.

## 10. Zusammenfassung

Die Ausgestaltung der Verkehrsdatenabfrage, der Ortung von Mobiltelefonen und der automatischen Kennzeichenfahndung weicht in den verschiedenen europäischen Ländern sehr stark voneinander ab. Während die Verkehrsdatenabfrage und die Handyortung in allen dargestellten Rechtsordnungen explizit geregelt sind, fehlt es in einigen Ländern an einer speziellen Ermächtigungsgrundlage für den Einsatz von automatischen Kennzeichenlese-systemen. Eine solche wird vielerorts als entbehrlich, die bestehenden Generalklauseln hingegen als ausreichend erachtet. Als Besonderheit ist hervorzuheben, dass der offene Einsatz von automatischen Kennzeichenlesesystemen nach britischem Verständnis mangels Privatsphäre in der Öffentlichkeit überhaupt keiner Ermächtigungsgrundlage bedarf.

Sofern spezielle Regelungen zum Einsatz von automatischen Kennzeichenlesesystemen bestehen, sind diese eher allgemein gehalten. Die Technik wird derzeit außer in Schweden und Finnland in allen aufgeführten Ländern eingesetzt – wenn auch in unterschiedlichem Umfang. In Schweden und Finnland werden die rechtlichen Gegebenheiten bzw. die technischen Möglichkeiten von automatischen Kennzeichenlesesystemen gegenwärtig evaluiert.

Die Abfrage von Verkehrsdaten und die Ortung von Mobiltelefonen haben sich in Europa wohl endgültig durchgesetzt. Auch wenn große Unterschiede im Hinblick auf Form und Inhalt der einschlägigen Regelungen bestehen, lassen sich doch einzelne Parallelen, bspw. die Zulässigkeit der Maßnahmen zur Abwehr einer Gefahr für Leib und Leben, feststellen.

Insbesondere im Hinblick auf die gegenwärtig auf europäischer Ebene geführte Diskussion um die Vorratsdatenspeicherung bleibt abzuwarten, inwiefern der Erlass einer neuen Richtlinie und deren Umsetzung durch die Mitgliedsstaaten Einfluss auf die Regelungen zur Verkehrsdatenabfrage und zur Handyortung haben wird. An der generellen Zulässigkeit dieser Maßnahmen wird sich voraussichtlich nichts ändern; durchaus denkbar sind jedoch Veränderungen bei deren Ausgestaltung und deren Stellenwert in der Praxis.

# Teil D: Rechtliche Bewertung der Maßnahmen

## 1. Verkehrsdatenabfrage

Bei der Verkehrsdatenabfrage handelt es sich um ein Instrument, das sowohl repressiv als auch präventiv zum Einsatz kommt. Die rechtlichen Rahmenbedingungen der Verkehrsdatenabfrage haben in den vergangenen Jahren einige Änderungen erfahren[175] und stehen seit der Entscheidung des BVerfG vom 2.3.2010 zur Vorratsdatenspeicherung[176] erneut in der Diskussion.[177] Die Kontroversen um eine mögliche Neuregelung beziehen sich vor allem auf die Bestimmungen des TKG und der StPO. Mittelbar ist freilich auch die Regelung des § 33b Abs. 6 S. 2 BbgPolG betroffen, die Rechtsgrundlage für die präventive Verkehrsdatenabfrage in Brandenburg. Denn in seinem Urteil vom 2.3.2010 macht das BVerfG, über die Fragestellungen zur Vorratsdatenspeicherung hinaus, auch einige Grundaussagen zu der Verkehrsdatenabfrage, die bei der Bewertung mit zu berücksichtigen sind.

Die Maßnahme kann grundsätzlich auch beiden Zwecken – Gefahrenabwehr und Strafverfolgung – gleichzeitig dienen. Diese präventiv-repressive Doppelnatur der Verkehrsdatenabfrage kommt speziell in Brandenburg darin zum Ausdruck, dass § 33b Abs. 8 BbgPolG eine Verwendung der präventiv erhobenen Daten für repressive Zwecke der Strafverfolgung ausdrücklich zulässt. Eine solche Zweckänderung lässt das BVerfG grundsätzlich zu.[178]

Festzustellen ist vorab schließlich, dass der Gesetzgeber in Brandenburg die Materie nicht vollständig autonom regeln kann. Da es sich bei § 33b Abs. 6 S. 2 BbgPolG, wie im Einleitungsteil ausgeführt[179], nur um eine Zugriffsnorm handelt, ist ihre Durchführbarkeit abhängig von den bundesrechtlichen Komplementärregelungen im TKG, die die Speicherung der Daten regeln. Hier ist die Entwicklung zur Zeit noch im Fluss. Aktuell existiert lediglich ein Eckpunktepapier des Bundesminsteriums der Justiz[180], das politisch allerdings umstritten ist.

### *1.1 Grundrechte der Teilnehmer*

#### *1.1.1 Das Fernmeldegeheimnis*

1.1.1.1 Daten über die Telekommunikation

Das Fernmeldegeheimnis schützt in erster Linie den Kommunikationsinhalt, umfasst aber gleichfalls die Umstände der Kommunikation. Dazu gehört insbesondere, ob, wann und wie

---

175 Siehe hierzu ausführlich *Kilchling* 2011.

176 BVerfG, 1 BvR 256/08 v. 2.3.2010, z.B. NJW 2010, S. 803, NStZ 2010, S. 341, NVwZ 2010, S. 770.

177 Siehe z.B. *Schramm/Wegener*, MMR 2011, S. 9; *Roßnagel*, NJW 2010, S. 1238.

178 BVerfG, 1 BvR 256/08 v. 2.3.2010, Abs. 236.

179 Vgl. Teil A, Pkt. 2.1.

180 http://www.bmj.de/SharedDocs/Downloads/DE/pdfs/Eckpunktepapier_zur_Sicherung_vorhandener_Verkehrsdaten_und_Gewaehrleistung_von_Bestandsdatenauskuenften_im_Internet.pdf?_blob=publicationFile

oft zwischen welchen Anschlüssen oder Endeinrichtungen Telekommunikationsverkehr stattgefunden hat oder versucht worden ist.[181] Demnach sind auch die Verkehrsdaten als Umstände der Telekommunikation vom Schutz des Fernmeldegeheimnisses erfasst. Die Auskunft über Verkehrsdaten greift somit in den Schutzbereich des Art. 10 GG ein.

Auch nicht verdächtige oder nicht gefährdete Telekommunikationsteilnehmer sind durch die Ermittlungsmaßnahme in ihren Rechten aus Art. 10 GG tangiert. Denn bei dem Nachweis der Telekommunikationsverbindungen werden auch die eingehenden Gespräche erfasst.[182] Damit wird zwangsläufig nicht nur der Anschluss des unmittelbar von der Maßnahme Betroffenen überprüft, sondern es werden auch Daten von unbeteiligten Dritten in die Maßnahme einbezogen. Denn alle Anschlüsse werden daraufhin untersucht, ob Verbindungen zu einem bestimmten Anschluss hergestellt worden sind. Insoweit handelt es sich um ein der Rasterfahndung vergleichbares Verfahren, das letztlich durch ein Ausschlussverfahren zu einem umfassenden Kommunikationsprofil der überwachten Personen führen kann.[183] Das Bundesverfassungsgericht hat den Eingriffscharakter bei den durch die Zielwahlsuche erfolgenden Zugriffen auf Telekommunikationsverkehrsdaten nicht verdächtiger Personen im Ergebnis allerdings als nicht grundrechtsrelevant eingestuft, da in der Praxis eine längerfristige Speicherung der Daten nur bei Treffern erfolgt.[184]

#### 1.1.1.2 Standortdaten

Nicht verdächtige bzw. unbeteiligte Telekommunikationsteilnehmer sind aber auch bei der Funkzellenabfrage in ihren Grundrechten betroffen. Bei einer Funkzellenabfrage werden sämtliche Daten der Mobilfunkkommunikation aus einem bestimmten Raum (Funkzelle, in die sich ein Mobiltelefon eingeloggt hat) erhoben. Dabei werden die Verbindungs- und Bestandsdaten auch unverdächtiger oder nicht als Zeugen in Betracht kommender Personen erfasst.[185] Hinsichtlich der Größenordnung der Erfassung von Daten Unbeteiligter kommt es darauf an, auf welchen Raum sich die Funkzellenabfrage bezieht. Wenn beispielsweise eine Abfrage für den Berliner Hauptbahnhof tagsüber erfolgt, werden mehr Menschen von der Funkzellenabfrage erfasst als bei der Abfrage in einer ländlichen Region. Aufschluss über Größenordnungen geben beispielsweise anlässlich einer Sitzung des Innen- und Rechtsausschusses des Schleswig-Holsteinischen Landtags erörterte Fälle von Funkzellenabfragen in

---

181 BVerfGE 67, S. 157, 172; BVerfGE 85, S. 386, 396; BVerfGE 100, S. 313, 358; BVerfG 1 BvR 330/96 v. 12.3.2003, S. 47; *Schäfer*, in: Löwe-Rosenberg, 2004, § 100g Rn. 3; *Leibholz/Rinck*, 2007, Art. 10, Rn. 31.

182 *Meyer-Goßner*, 2006, § 100g Rn. 11.

183 *Weßlau*, ZStW 113 (2001), S. 693; kritisch unter Hinweis auf eine wegen bloßer Willkürkontrolle durch Revisionsgerichte nur unzureichenden Wirkung der Subsidiaritätsklausel des § 100 g II StPO *Wolter*, in: SK StPO, 2006, § 100g, Rn. 8.

184 BVerfG NJW 2003, S. 1787, 1793 unter Verweis auf BVerfGE 100, S. 313, 366.

185 *Schäfer*, in: Löwe-Rosenberg, 2004, § 100g Rn. 28.

Ermittlungsverfahren wegen Brandstiftungs- und Tötungsdelikten.[186] Danach waren in einem Brandstiftungsverfahren etwa 700 Personen, die Mobiltelefone in einer relevanten Funkzelle zu einer bestimmten Zeit benutzt hatten, in die Ermittlungen einbezogen worden; in einem Verfahren wegen eines Tötungsdelikts waren mindestens 120 Mobilfunknutzer betroffen. Die Betroffenen, so wird in der parlamentarischen Debatte hervorgehoben, befanden sich erwartungsgemäß zunächst in einer Lage, in der durch zusätzliche Ermittlungen untersucht wurde, ob sie als Tatverdächtige, Zeugen oder eben als Nichtverdächtige oder Unbeteiligte im polizeirechtlichen Sinne in Betracht kommen.

### *1.1.2 Verfassungsrechtliche Legitimation*

Eingriffe in das Fernmeldegeheimnis verlangen zunächst eine förmliche gesetzliche Grundlage.[187] Diese ist vorliegend in § 33b Abs. 6 S. 2 BbgPolG. Wie bei jedem staatlichen Eingriff muss jedoch auch bei der Verkehrsdatenabfrage die Verhältnismäßigkeit gewahrt sein. Gerade wegen der hohen Anzahl an unbeteiligten Betroffenen wurde im Gesetz die Verhältnismäßigkeit durch das Erfordernis der Subsidiarität für die Funkzellenabfrage und die Zielwahlsuche konkretisiert. Gerade bei einer verdeckten Ermittlungsmethode, die eine Vielzahl von Personen betrifft, spielt die Verhältnismäßigkeitsprüfung eine ausschlaggebende Rolle. Sie sichert die Schaffung eines Gleichgewichts zwischen der durch die Ermittlungsmaßnahme geförderten Sicherheit der Bürger und der dadurch gleichzeitig bewirkten Einschränkung der Grundfreiheiten.

Die Verhältnismäßigkeit setzt die Eignung der Maßnahme zur Verfolgung eines legitimen Zweckes voraus. Legitimer Zweck der Maßnahme ist die Gefahrenabwehr, die dem Ziel des Rechtsgüterschutzes dient. Näher differenziert wird die Legitimität des Schutzzwecks durch die Bestimmung der Einzelziele, die mit der konkreten Maßnahme verfolgt werden. Geeignet ist die Maßnahme dann, wenn das vom Staat gewählte Mittel zur Erreichung des konkreten Zwecks tauglich ist.[188] Regelungen hierzu fehlen in § 33b Abs. 6 S. 2 BbgPolG in der gegenwärtig normierten Form jedoch. Auch aus dem Normzusammenhang mit den anderen Bestimmungen des § 33b BbgPolG wird eine explizite Zweckbestimmung nicht erkennbar. Daher erscheint insoweit eine Überarbeitung angezeigt.

Eine solche Neuregelung sollte sich eng an den Vorgaben orientieren, die das BVerfG in dem Urteil vom 2.3.2010 entwickelt hat.[189] Danach ist ein präventiver Zugriff zulässig zur Abwehr von Gefahren für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder zur Abwehr einer gemeinen Gefahr[190]. Dabei

---

186 Schleswig-Holsteinischer Landtag Stenographischer Dienst und Ausschussdienst, Niederschrift, Innen- und Rechtsausschuss, 16. WP - 5. Sitzung, 7. September 2005, S. 4 ff.

187 *Dreier*, in: Dreier, 2004, Art. 2 I Rn. 86.

188 *Dreier*, in: Dreier, 2004, Vorb. Rn. 147.

189 BVerfG, 1 BvR 256/08 v. 2.3.2010, Abs. 230, 231.

190 Die gemeine Gefahr ist z.B. in Art. 13 Abs. 4 GG und in § 31 PolG-BW normiert.

müssen tatsächliche Anhaltspunkte einer konkreten Gefahr für die schutzwürdigen Rechtsgüter vorliegen.

Die Ausführungen des BVerfG im Kontext des Urteils zur Vorratsdatenspeicherung beziehen sich unmittelbar allerdings nur auf Verkehrsdaten, die umfassend und für längere Zeit gespeichert werden. Unberührt bleibt der allgemeine Grundsatz, dass der Gesetzgeber durch geeignete Rahmenregelungen die Verhältnismäßigkeit aktiv steuern kann.[191] So wurde in dem Urteil des BVerfG zur Kennzeichenfahndung die Bestimmung des § 36a BbgPolG mit seiner spezifischen Kombination aus weit gefasstem Verwendungszweck bei gleichzeitig eng begrenzten Eingriffsvoraussetzungen als positives Beispiel einer verhältnismäßigen Rechtsgrundlage herausgestellt.[192] Möglich wäre daher beispielsweise, die Zugriffsmöglichkeiten auf Standortdaten zu begrenzen. Denn im Bereich der Gefahrenabwehr werden die anderen Datenarten regelmäßig nur eine sehr begrenzte Relevanz haben. Eine solche Beschränkung könnte im Gegenzug eine Erweiterung des Einsatzspektrums auf weitere Gefahrensituationen erlauben. Weitere Begrenzungen in Form einer Beschränkung auf Echtzeitdaten oder Daten aus einem bestimmten, zeitlich vordefinierten Zeitraum erscheint ebenfalls denkbar. Ob dies auch polizeitaktisch sinnvoll wäre, kann hier nicht beurteilt werden.

Anders als die Vorschrift des § 100g StPO sieht § 33b Abs. 6 S. 2 BbgPolG einen Richtervorbehalt nicht vor. Auch dies steht nicht im Einklang mit den Grundsätzen des BVerfG aus dem Urteil zur Vorratsdatenspeicherung. Zur verfahrensrechtlichen Absicherung des Grundrechtsschutzes fordert das Gericht vielmehr ausdrücklich, dass die Abfrage von Verkehrsdaten grundsätzlich unter Richtervorbehalt zu stellen ist. [193]

Diese Lücke hat das Ministerium des Innern erkannt und am 14.7.2010 einen Erlass zur Auslegung des § 33b Abs. 6 S. 2 BbgPolG herausgegeben.[194] Dieser greift den erwähnten Mangel auf und stellt die Verkehrsdatenabfrage grundsätzlich unter den Vorbehalt richterlicher Anordnung. Ausnahmen lässt der Erlass lediglich bei Gefahr im Verzug in folgenden Situationen zu:

- bei Beseitigung einer Suizidgefahr,
- bei der Suche nach gefährdeten Vermissten,
- bei der Suche nach minderjährigen Vermissten oder
- bei der Befreiung aus hilfloser Lage.

Gefahr im Verzug ist nur zu bejahen, wenn aufgrund der Prüfung im Einzelfall die Zeit fehlt, vor dem Auskunftsersuchen einen Richter zu erreichen. In diesen Fällen ist die richterliche Entscheidung unverzüglich nachzuholen.

---

191 Vgl. *Roßnagel*, NJW 2010, S. 1242.

192 BVerfG, 1 BvR 2074/05 u. 1 BvR 1254/07 v. 11.3.2008, Abs. 230, 183.

193 BVerfG, 1 BvR 256/08 v. 2.3.2010, Abs. 247.

194 Siehe Teil G, Anhang 4.

Diese Beschränkungen des grundsätzlichen Richtervorbehaltes erscheinen im Hinblick auf den hohen Stellenwert der Rechstgüter Leben und körperliche Unversehrtheit sachgerecht. Werden sie in dieser Form in Gesetzesform übertragen, kann an der Verhältnismäßigkeit der Rechstgrundlage kein Zeifel mehr bestehen.

Durch eine solche Regelung werden im Übrigen Diskrepanzen zu den Voraussetzungen vermieden, die für repressive Verkehrsdatenabfragen gem. § 100g StPO gelten. Unterschiedliche Regelungen zum Richtervorbehalt könnten ansonsten zu rechtlichen Problemen führen, wenn Verkehrsdaten, die auf der Grundlage von § 33b Abs. 6 S. 2 BbgPolG erhoben wurden, gem. § 33b Abs. 8 BbgPolG an die Strafverfolgungsbehörden weitergegeben werden sollen.

#### *1.1.2 Das Recht auf informationelle Selbstbestimmung*

Da Art. 10 GG als spezielles Grundrecht vorgeht, kommt für die Verkehrsdatenabfrage das Recht auf informationelle Selbstbestimmung (Art. 2 I i.V.m. 1 I GG) nicht in Betracht.[195]

### *1.2 Grundrechte der Telekommunikationsanbieter*

Von den Anordnungen zur Verkehrsdatenabfrage könnten auch Rechte der Telekommunikationsanbieter betroffen sein. Gemäß § 33b Abs. 6 S. 2 BbgPolG sind die Diensteanbieter zur Auskunftserteilung verpflichtet. Dies könnte als Eingriff in Art. 12 GG und Art. 14 GG gewertet werden. Gemäß Art. 19 Abs. 3 GG sind die Art. 14 Abs. 1 GG und 12 Abs. 1 GG auch auf juristische Personen anwendbar.

#### *1.2.1 Die Berufsfreiheit*

Die gesetzliche Pflicht der Telekommunikationsanbieter, Auskunft über lediglich zu Rechnungszwecken gespeicherte Daten zu erteilen, könnte die in Art. 12 GG verbürgte Freiheit, die Art und Weise der Berufsausübung selbst zu bestimmen, beeinträchtigen. In der Rechtsprechung des Bundesverfassungsgerichts wird unterstrichen, dass sich die Indienstnahme Privater für öffentliche Aufgaben auch am Maßstab des Art. 12 Abs. 1 GG messen lassen muss.[196] Allerdings hat das BVerfG nunmehr entschieden, dass die Pflicht zur Vorratsdatenspeicherung die betroffenen Unternehmen nicht in ihren Grundrechten aus Art. 12 GG verletzt.[197] Die Pflichten werden weder hinsichtlich ihres technischen Aufwandes noch hinsichtlich der damit verbundenen finanziellen Belastungen als unverhältnismäßig bewertet.[198]

---

195 BVerfG, 1 BvR 256/08 v. 2.3.2010, Abs. 191.

196 BVerfGE 30, S. 292, 311; BVerfGE 85, S. 329, 334.

197 BVerfG, 1 BvR 256/08 v. 2.3.2010, Abs. 293f.

198 BVerfG, 1 BvR 256/08 v. 2.3.2010, Abs. 296.

*1.2.2 Das Eigentumsrecht*

Art. 14 Abs. 1 GG schützt nicht nur die unmittelbare Herrschaft über den Eigentumsgegenstand, sondern auch Verfügungsfreiheit und Privatnützigkeit.[199] Zur Umsetzung der Pflicht der Übermittlung von Verkehrsdaten an Strafverfolgungsbehörden müssen aber Telekommunikationsanbieter in Hardware und Software investieren. Dabei handelt es sich um die Herstellung einer Infrastruktur zur Überwachung sowie deren dauerhafte Unterhaltung und Anpassung an technologische Entwicklungen. Sind die entsprechenden, zur Überwachung geeigneten Einrichtungen vorhanden, so müssen diese nach Maßgabe der gesetzlichen Vorschriften genutzt werden.[200] Insoweit betrifft die Pflicht zur Anpassung des Betriebs an Erfordernisse der Überwachung und die Pflicht zur Übermittlung von Verkehrsdaten die im Schutzbereich des Eigentums liegende Eigentumsnutzungsfreiheit.

Ob dies einen unzulässigen Eingriff in Art. 14 Abs. 1 GG mit sich bringt, ist umstritten.[201] Für die Beurteilung von Eingriffen in Art. 14 GG geht es jedoch – wie bei Eingriffen in die Berufsfreiheit – prinzipiell um die Verhältnismäßigkeit.[202] Grundsätzlich ist die Heranziehung Privater zur Erfüllung originär staatlicher Aufgaben nach einhelliger Auffassung zulässig[203], wenn vernünftige Erwägungen des Gemeinwohls die Heranziehung begründen. Herausragende Gemeinwohlbelange werden mit dem Ziel einer effektiven Strafverfolgung selbstverständlich angestrebt.[204] Eine besondere und die Verpflichtung zu Leistungen begründende Stellung der Telekommunikationsunternehmen folgt aus ihrer ausschließlichen Verfügungsmacht über Netze und Speichermedien. Im Übrigen wird auch das Interesse an einem wirksamen Geheimnisschutz genannt[205]. Die ausschließliche Verfügungsmacht sowie der Schutz der Daten der Kunden rechtfertigen daher die Indienstnahme der Telekommunikationsunternehmen als private Rechtssubjekte.[206] Die Grenze des verfassungsrechtlich Zulässigen ergibt sich aus dem Grundsatz der Verhältnismäßigkeit.[207] Umstritten ist allerdings die Frage, ob die Auferlegung der Kosten für die Vorhaltung der Infrastruktur der Überwachung sowie für die beständige Anpassung der Überwachungsinfrastruktur an den Stand der Technik entschädigungslos erfolgen darf. Hier werden keine anderen Maßstäbe anzulegen sein als im Rahmen von Art. 12 GG. Auch insoweit ist ein ungerechtfertigter Eingriff daher abzulehnen. Im Übrigen gewährt § 33b Abs. 6 S. 3 BbgPolG zumindest eine moderate Entschädigung gem. § 23 JVEG.

---

199 *Schmidt-Preuß*, 2005, S. 8.

200 *Schmidt-Preuß*, 2005, S. 8.

201 *Hammerstein*, MMR 2004, S. 223; *Kube/Schütze*, CR 2003, S. 667.

202 *Hammerstein*, MMR 2004, S. 223.

203 BVerfGE 30, S. 292, 311; zusammenfassend *Schmidt-Preuß*, 2005, S. 29.

204 *Hammerstein*, MMR 2004, S. 224.

205 *Welp*, 2000, S. 136.

206 *Dorsch*, 2005, S. 33; *Welp*, 2000, S. 136.

207 BVerfGE 30, S. 292, 311; BVerfGE 85, S. 329, 334; *Hammerstein*, MMR 2004, S. 223; *Welp*, 2000, S. 135.

## 2. Ortung von Mobiltelefonen

Anders als Verkehrsdaten fallen Daten, die beim Einsatz des IMSI-Catchers erhoben werden, nicht in den Schutzbereich des in Art. 10 Abs. 1 GG verankerten Fernmeldegeheimnisses.[208] Nach ständiger Rechtsprechung schützt das Fernmeldegeheimnis den Inhalt und die Umstände einer mittels Telekommunikationseinrichtung durchgeführten Kommunikation.[209] Eine Kommunikation liegt nur dann vor, wenn Inhalte zwischen zwei Personen ausgetauscht werden.[210] Neben dem Inhalt der Telekommunikation werden zwar auch die näheren Umstände des Fernmeldevorgangs geschützt, jedoch nur, soweit sich diese in irgendeiner Weise auf Kommunikationsinhalte beziehen. Als solche Umstände mit Inhaltsbezug gelten insbesondere Angaben dazu, zwischen wem wann und wie oft ein Telekommunikationsverkehr stattgefunden hat oder versucht wurde.[211] Sofern sich ein Mobiltelefon im Stand-By-Betrieb befindet, findet nur eine Kommunikation technischer Geräte, nicht aber eine von Art. 10 Abs. 1 GG geschützte individuelle Kommunikation zwischen Personen statt.[212] Zudem haben die beim Einsatz von IMSI-Catchern ermittelten Standortdaten keinen inhaltlichen Bezug zum Telekommunikationsvorgang. Sie dienen lediglich der Betriebsbereitschaft des Mobiltelefons. Rückschlüsse auf Telekommunikationsbeziehungen und -inhalte können daraus hingegen nicht gezogen werden. Mangels menschlich veranlassten Kommunikationsvorgangs fällt der Einsatz von IMSI-Catchern nicht in den Schutzbereich von Art. 10 Abs. 1 GG. In Betracht kommt lediglich ein Eingriff in das durch Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG gewährleistete Recht auf informationelle Selbstbestimmung sowie die allgemeine Handlungsfreiheit.[213]

## 3. Anlassbezogene automatische Kennzeichenfahndung

Maßgeblich für die rechtliche Bewertung der Maßnahme ist die Prüfung, ob und in welchen Fällen in grundrechtlich geschützte Positionen eingegriffen und ob und unter welchen Umständen ein solcher Eingriff verhältnismäßig und damit zulässig ist. Die Zulässigkeit der automatischen Kennzeichenfahndung in der Regelungsvariante des § 36a BbgPolG ist danach an dem (Grund-)Recht auf informationelle Selbstbestimmung zu messen. Liegt ein solcher Eingriff vor, muss in einem weiteren Schritt geprüft werden, ob und unter welchen Voraussetzungen dieser gerechtfertigt ist. Dabei muss jede Eingriffsvariante gesondert betrachtet und evaluiert werden.

---

208 BVerfG MMR 2006, 805, 806.

209 BVerfGE 107, 299, 312; vgl. auch *Löffelmann*, AnwBL 2006, 598.

210 *Roggan*, KritV 2003, 76, 80.

211 BVerfG MMR 2006, 805, 806; vgl. auch *Nachbaur*: Standortfeststellung und Art. 10 GG – Der Kammerbeschluss des BVerfG zum Einsatz des „IMSI-Catchers", NJW 2007, 335, 337; *Löffelmann*: AnwBL 2006, 598.

212 BVerfG MMR 2006, 805, 806; *Bär*: Telekommunikationsüberwachung und andere verdeckte Ermittlungsmaßnahmen – Gesetzliche Neuregelungen zum 01.01.2008, in: MMR 2008, 215.

213 BVerfG MMR 2006, 805, 807 f.; vgl. auch *Löffelmann*: AnwBL 2006, 598. 600; kritisch *Nachbaur*: Standortfeststellung und Art. 10 GG – Der Kammerbeschluss des BVerfG zum Einsatz des „IMSI-Catchers", NJW 2007, 335 ff.; vgl. auch *Löffelmann*: AnwBL 2006, 599.

### *3.1 Das Recht auf informationelle Selbstbestimmung*

Das Recht auf informationelle Selbstbestimmung hat seinen Ausgangspunkt bekanntlich in dem sog. Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983[214] und wurde seither kontinuierlich weiterentwickelt.[215] Es schützt die Befugnis des Einzelnen, „grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden".[216]

Durch die elektronische Datenverarbeitung ist es technisch möglich geworden, Daten unbegrenzt zu speichern und sie „jederzeit ohne Rücksicht auf Entfernungen in Sekundenschnelle" abzurufen. Ferner könnten die gespeicherten Daten automatisch „zu einem teilweise oder weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden, ohne dass der Betroffene dessen Richtigkeit und Verwendung zureichend kontrollieren kann". Es muss also nicht mehr „wie früher auf manuell zusammengetragene Karteien und Akten zurückgegriffen werden".[217] Die Möglichkeiten, welche die moderne Datenverarbeitung bietet, seien in weiten Bereichen nur noch für Fachleute durchschaubar und könnten daher beim Staatsbürger die „Furcht vor einer unkontrollierbaren Persönlichkeitserfassung" auslösen.[218] Aus diesem Grund sei die Befugnis des Einzelnen, selbst über die Offenbarung persönlicher Lebenssachverhalte zu entscheiden, besonders gefährdet. Der Einzelne müsse daher vor der unbegrenzten Erhebung, Speicherung, Verwendung und Weitergabe seiner Daten geschützt werden.[219] Das Recht auf informationelle Selbstbestimmung als besondere Ausprägung des allgemeinen Persönlichkeitsrechts soll diesen Schutz gewährleisten und sicherstellen, dass der Einzelne auch in Zukunft selbst über die Verwendung personenbezogener Daten entscheiden kann. Dies dient dem Wert und der Würde des Einzelnen[220], wie sie in Art. 1 Abs. 1 GG verankert sind und damit an der Spitze der Verfassung stehen. Bei dem Recht auf informationelle Selbstbestimmung handelt es sich also um ein Selbstbestimmungsrecht über personenbezogene Informationen[221], welches vor allem auch im Hinblick auf die neuen Möglichkeiten der elektronischen Datenverarbeitung und die damit verbundenen Risiken entwickelt wurde.[222]

Bei der automatischen Kennzeichenfahndung werden die Kennzeichen der vorbeifahrenden Kraftfahrzeuge ausgelesen und mit dem jeweiligen Fahndungsbestand abgeglichen. Neben

---

214 BVerfGE 65, 1 (Volkszählungsurteil).

215 Zuletzt BVerfGE BvR 370/07 und 1 BvR 595/07 vom 27.02.2008 (Online-Durchsuchung), BVerfG 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008 (Automatische Kennzeichenfahndung), BVerfGE 2 BvR 1372/07 und 2 BvR 1745/07 vom 17.02.2009 (Kreditkartenfahndung – Aktion Mikado), BVerfGE BvR 256/08, 1 BvR 263/08 und 1 BvR 586/08 vom 02.03.2010 (Vorratsdatenspeicherung).

216 BVerfGE 65, 1, 42.

217 BVerfGE 65, 1, 42.

218 BVerfGE 65, 1, 4.

219 BVerfGE 65, 1, 43.

220 BVerfGE 65, 1, 4.

221 *Maunz/Dürig-Di Fabio*, Art. 2 Rn. 175; Vogelgesang, S. 23.

222 *Dreier*, Art. 1 Rn. 52.

dem Kennzeichen wird dabei erhoben, wann das Fahrzeug die Kontrolleinrichtung passiert hat und in welche Richtung es gefahren ist. Ferner wird von dem Fahrzeug ein Foto angefertigt.[223] Dabei handelt es sich um Einzelangaben über persönliche und sachliche Verhältnisse des Fahrers bzw. des Fahrzeughalters und damit um personenbezogene Daten im Sinne des § 3 Abs. 1 BDSG. Diese werden zum Zwecke des Abgleichs mit dem Fahndungsbestand von einer staatlichen Stelle erhoben, verarbeitet und im Nichttrefferfall wieder gelöscht. Die automatische Kennzeichenfahndung ist daher eine Maßnahme, die in den Schutzbereich des Grundrechts auf informationelle Selbstbestimmung fällt.[224] Dem steht auch nicht entgegen, dass das Kennzeichen gerade zur Identifizierung dient[225] und die Halterdaten mittels einer sog. einfachen Registerauskunft nach § 39 Abs. 1 StVG vergleichsweise leicht erlangt werden können.[226] Die Einsichtnahme in das Fahrzeugregister und die Beauskunftung entsprechender Anfragen ist von einem berechtigten Interesse abhängig, sodass es sich bei diesem Register um keine allgemein zugängliche Quelle handelt.[227]

Unproblematisch ist hingegen die Bildaufnahme. Das Foto wird aus der Rückenperspektive angefertigt und zeigt lediglich Konturen. Insassen sind in der Regel nicht zu erkennen und wären wegen der Rückansicht ohnehin nicht identifizierbar. Solche Fälle hat das BVerfG explizit für unbedenklich erklärt.[228]

### *3.2. Eingriff in das Recht auf informationelle Selbstbestimmung*

Zu prüfen ist, ob die automatische Kennzeichenfahndung auch einen Eingriff in das Recht auf informationelle Selbstbestimmung darstellt.

Bei Durchführung der Maßnahme werden diverse Daten über den Fahrer bzw. den Halter des Fahrzeuges erhoben, ohne dass sich der Betroffene dagegen wehren kann. Wird die Maßnahme mit einem stationären System durchgeführt und ist dem Betroffenen bekannt, wo diese errichtet sind, kann er die Erfassung lediglich vermeiden, indem er auf andere, nicht überwachte Verkehrswege ausweicht und dadurch die Kontrollstelle meidet. Ist dem Fahrer die Existenz oder der Standort der Lesegeräte nicht erkennbar, was bei den stationären Anlagen der Regelfall sein dürfte, hat er keine Möglichkeit, sich der Maßnahme zu entziehen. Wiederholt weist das Bundesverfassungsgericht darauf hin, dass das Recht auf informationelle

---

223 Siehe Teil A, Pkt. 2.3.

224 Vgl. *Cornils*, Jura 2010, 443, 445; *Robrecht*, NJ 2008, 9, 10; *Hornmann*, NVwZ 2007, 669, 670; *Arzt*, SVR 2004, 321, 323.

225 BVerfG vom 11.03.2008, Abs. 83.

226 Arzt, SVR 2004, 321, 323.

227 BGH NJW 2003, 226, 327.

228 BVerfG 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008, Abs. 89

Selbstbestimmung auch vor derartigen Gefährdungen der Verhaltensfreiheit schützen soll, die durch die Erhebung und Verarbeitung von Daten entstehen können.[229]

Ein Eingriff in das Recht auf informationelle Selbstbestimmung liegt grundsätzlich bereits in der Erhebung von personenbezogenen Daten, sofern diese den Behörden verfügbar gemacht werden und einem anschließenden Abgleich mit anderen Datenbeständen dienen können.[230] Der grundrechtliche Schutz entfällt nicht schon allein aufgrund der Tatsache, dass die jeweiligen Informationen allgemein zugänglich sind. Vielmehr schützt das Recht auf informationelle Selbstbestimmung auch das Interesse des Einzelnen, dass seine Daten nicht im Rahmen einer automatisierten Informationserhebung zwecks Speicherung und Weiterverwertung erhoben werden.[231]

Andererseits lehnt das Bundesverfassungsgericht das Vorliegen eines Eingriffs ab, wenn Daten unmittelbar nach ihrer Erfassung wieder spurlos und anonym ausgesondert werden, ohne dass die Möglichkeit besteht, einen Personenbezug herzustellen.[232] Entscheidend ist, ob sich das behördliche Interesse an den jeweiligen Daten bei einer Gesamtbetrachtung „bereits derart verdichtet hat, dass ein Betroffensein in einer den Grundrechtseingriff auslösenden Qualität zu bejahen ist“[233].

Bei der automatischen Kennzeichenfahndung sind drei denkbare Konstellationen zu unterscheiden:

- die Nichttrefferfälle
- die Trefferfälle
- und die Fehltreffer.[234]

In einem Nichttrefferfall wird das fragliche Kennzeichen zwar von der Kontrolleinrichtung erfasst und im Arbeitsspeicher mit dem Fahndungsbestand abgeglichen, der Abgleich führt aber zu dem Ergebnis, dass das eingelesene Kennzeichen nicht mit dem gesuchten identisch ist. Die Daten werden dann verworfen, d.h. unwiderruflich gelöscht, sodass die erhobenen Daten nicht mehr rekonstruiert werden können. Eine Individualisierung, d.h. eine (nachträgliche) Herstellung eines konkreten Personenbezuges, ist nicht mehr möglich. Ein Grundrechts-

---

229 Siehe insbesondere BVerfG 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008, Rn. 66, 77 ff.; BVerfGE 65, 1, 43; *Roßnagel*, NJW 2008, 2547, 2548.

230 BVerfG 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008, Abs. 60; vgl. auch BVerfGE 100, 313, 366; 115, 320, 343.

231 BVerfG 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008, Abs. 67.

232 BVerfG 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008, Abs. 68; BVerfGE 107, 299, 328. In BVerfGE 100, 313, 366; 115, 320, 343 wurde ein Eingriff abgelehnt, wenn Daten „ungezielt und allein technikbedingt ... miterfasst“ worden waren.

233 BVerfG 2 BvR 1447/10 vom 12.08.2010, Rn. 16; BVerfG 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008, Abs. 65; BVerfGE 115, 320, 343.

234 Siehe auch Teil A, Pkt. 2.3.

eingriff findet daher nicht statt; denn die Herstellbarkeit des Personenbezuges ist die entscheidende Grenze, ab der das BVerfG einen Grundrechtseingriff annimmt.[235]

Die Situation gleicht der des „sehenden aber vergessenden Polizisten", der am Straßenrand steht und zur Fahndung nach einem einzelnen Kennzeichen, das er sich gemerkt hat, einen Blick auf alle vorbeifahrenden Kennzeichen wirft. Der Polizist wäre nicht einmal dazu in der Lage, sich alle Kennzeichen zu merken. Vielmehr würde er gezielt nach dem einen Fahrzeug mit dem entsprechenden Kennzeichen Ausschau halten. Dasselbe läuft bei Durchführung einer automatischen Kennzeichenfahndung ab. Ein Unterschied besteht lediglich darin, dass anstatt des menschlichen Auges die elektronische Datenverarbeitung eingesetzt wird und auf diese Weise mehr Kennzeichen mit einem deutlich größeren Fahndungsbestand abgeglichen werden können.[236] In Anbetracht der ständig steigenden Verkehrsdichte[237] und immer knapper werdenden Personalressourcen wäre ein äquivalenter Einsatz von personellen Kräften nicht realisierbar.[238] Um die Vergleichbarkeit mit dem „vergessenden" Polizisten zu wahren, muss jedoch rechtlich und technisch sichergestellt werden, dass die erfassten Kennzeichen unverzüglich mit dem Fahndungsbestand abgeglichen und alle erhobenen Daten im Nichttrefferfall sofort und unwiderruflich gelöscht werden, ohne dass die Möglichkeit besteht, einen Personenbezug herzustellen. Wird diesen Anforderungen genügt, ist weder eine serielle Erfassung von personenbezogenen Daten noch eine Verwendung der erhobenen Daten durch staatliche Stellen ohne Zustimmung des betroffenen Bürgers möglich. Ein Eingriff in das Recht auf informationelle Selbstbestimmung kann dann nicht angenommen werden.[239]

Liegt ein Trefferfall vor, werden die erfassten Daten gespeichert und zunächst an den lokalen Rechner (bei mobilen Einsätzen) bzw. (bei stationären Einsätzen) den Zentralrechner übermittelt – unabhängig davon, ob es sich um einen „echten" Trefferfall oder einen sog. Fehltreffer handelt. Bei Eingang der Treffermeldung führt der zuständige Polizeibeamte einen manu-

---

235 So auch BVerfG, 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008, Abs. 68.

236 So auch der Landtag und die Landesregierung von Schleswig-Holstein in BVerfG, 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008, Abs. 52. Diese weisen darauf hin, dass die Effektivierung einer Fahndung nicht rechtswidrig sein könne, solange die Fahndung selbst auch rechtswidrig sei.

237 Vgl. Pressemitteilung des Statistischen Bundesamtes Nr. 034 vom 26.01.2011.

238 A.A. *Robrecht*, NJ 2008, 9, 11, der der Meinung ist, dass diese Ansicht „den durch die moderne Technik bedingten ‚Quantitäts- und Qualitätssprung', mit dem die menschlichen Wahrnehmungsmöglichkeiten durch technische Mittel verlängert und wesentlich erweitert werden", verkenne. Schließlich werde eine „ungleich *höhere* Zahl von Bürgern ‚ins Visier' genommen". Dem ist jedoch nicht zuzustimmen. Auch das menschliche Auge versucht, möglichst alle Fahrzeuge zu erfassen, ist dazu aufgrund des erhöhten Verkehrsaufkommens jedoch nicht mehr in der Lage. Es handelt sich also lediglich um eine Effektivierung der seit jeher durchgeführten Verkehrsüberwachungen.

239 BVerfG, 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008, Abs. 68; Frenz, DVBl. 2009, 333, 337; vgl. auch BVerfG 2 BvR 1447/10 vom 12.08.2010, Rn. 6; *Bücken*, jurisPR-VerkR 20/2010, Anm. 4. A.A. *Arzt*, DÖV 2005, 56, 58; Vgl. *Bodenbenner/Heinemann*, NVwZ 2010, 679, 681; *Breyer*, NVwZ 2008, 824, 827; *Schieder*, NVwZ 2004, 778, 781. *Lang*, JurPC Web-Dok. 93/2005, Abs. 83 ist der Ansicht, dass „Eingriffe in das Recht auf informationelle Selbstbestimmung ... innerhalb der Datenverarbeitungsanlage stattfinden"; *Robrecht*, NJ 2008, 9, 10, spricht von einem „Massengrundrechtseingriff".

ellen Abgleich der übermittelten Daten mit dem Fahndungsbestand durch. Handelt es sich um einen Fehltreffer, müssen sämtliche Daten zu dem entsprechenden Fahrzeug ausgesondert und gelöscht werden.

Fraglich ist, ob die Übermittlung der erhobenen Daten an die zuständige Polizeidienststelle samt manueller Überprüfung bereits einen Eingriff in das Recht auf informationelle Selbstbestimmung begründet oder nicht. Für einen Eingriff würde sprechen, dass die erfassten Daten durchaus – wenn auch nur kurzfristig – von der Polizei gespeichert und jeglicher Einflussnahme des betroffenen Bürgers entzogen werden. Die Daten werden den staatlichen Behörden also zwecks manuellem Abgleich verfügbar gemacht. Nichts anderes geschieht jedoch, wenn ein Polizist ein Kennzeichen visuell wahrnimmt, es manuell in einen Computer eingibt oder auf einem Zettel notiert. Auch in diesen Fällen werden die Daten kurzzeitig dem Einflussbereich des betroffenen Bürgers entzogen. Sofern sichergestellt ist, dass die erhobenen Daten nach dem manuellen Abgleich im Fall eines Fehltreffers sofort und unwiderruflich gelöscht werden, unterscheidet sich das Vorgehen qualitativ nicht von jenem in einem Nichttrefferfall. Im Rahmen des manuellen Abgleichs wird lediglich mit menschlichen Sinnen wiederholt, was vorweg schon einmal automatisiert abgelaufen ist: Das erfasste Kennzeichen wird mit dem Fahndungsbestand, der nunmehr auf einen einzelnen Datensatz komprimiert ist, abgeglichen.

So ist es hier. Die Überprüfung ist Teil des bereits in Gang gesetzten Abgleichvorganges; es werden keine neuen Daten erhoben und die vorhandenen Daten auch nicht umgewandelt oder aufgeschlüsselt. Im Moment der Überprüfung des Kennzeichens handelt es sich nach wie vor um ein anonymes, aggregiertes Datum. Der jeweilige Beamte überprüft lediglich die Übereinstimmung anhand abstrakter Parameter (Buchstaben-Zahlen-Abfolge), ohne dass eine weitergehende gedankliche Individualiserung in Form einer Zuordnung zu Halter- oder Fahndungsdaten erfolgt. Der Vorgang kann sachlich mit dem Lesen oder der sonstigen optischen Kenntnisnahme einer Liste mit unbekannten Telefon- oder Kreditkartennummern verglichen werden. Für eine solche Konstellation hat das BVerfG in seinem Nichtannahmebeschluss zu der Operation Mikado bereits einen Eingriff abgelehnt.[240] Ziel des manuellen Abgleichs ist es gerade, sicherzustellen, dass kein Fehltreffer gespeichert und die Daten eines falschen Betroffenen in das Risiko der Deanonymisierung geraten. Der Polizeibeamte weiß im Moment der Überprüfung nicht, wem das Kennzeichen gehört, und er will es auch gar nicht wissen. Die verfassungsrechtlich relevante Grenze zum Grundrechtseingriff ist damit noch nicht überschritten. Vielmehr stärkt die Überprüfung den Grundrechtsschutz, indem es ungerechtfertigte Folgemaßnahmen abwendet. Die Überprüfung von Kennzeichen ohne Individualisierung entspricht vom Ablauf her weitgehend der automatisierten Durchsuchung. Fehltreffer werden sodann unverzüglich gelöscht. An dieser Stelle verlangt das BVerfG allerdings die unverzügliche Überprüfung und nachfolgende sofortige Löschung der Fehltreffer.[241] Die Vorschrift des § 36a BbgPolG sollte entsprechend angepasst werden.

---

[240] BVerfGE 2 BvR 1372/07 und 2 BvR 1745/07 vom 17.02.2009.

[241] BVerfG, 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008, Leitsatz 1 u. Abs. 62.

Nur wenn der manuelle Abgleich zu dem Ergebnis führt, dass das erfasste Kennzeichen tatsächlich im Fahndungsbestand enthalten ist, und die Treffermeldung als solche bestätigt wird, werden die erhobenen Daten gespeichert, verarbeitet und gegebenenfalls Grundlage weitergehender Maßnahmen. Ab diesem Zeitpunkt stehen die Daten den staatlichen Behörden jederzeit zur Verfügung und können auch ohne Einwilligung des Betroffenen verwendet werden. Insbesondere ist es den staatlichen Behörden nun ohne weiteres möglich, den Fahrzeughalter und gegebenenfalls auch den Fahrer zu ermitteln und auf diese Weise einen Personenbezug herzustellen. Sobald die erhobenen Daten gespeichert werden, liegt daher ein Eingriff in das Recht auf informationelle Selbstbestimmung vor.[242]

Einen Sonderfall stellt daneben der Einsatz eines Erfassungssystems zur Verkehrszählung dar. Wie eingangs beschrieben, wird von dieser Möglichkeit in Brandenburg mitunter zur Einsatzplanung Gebrauch gemacht.[243] So kann beispielsweise gezählt werden, wie viele Fahrzeuge eine bestimmte Stelle passieren. Ziel ist gerade nicht die Identifizierung Einzelner nach individuellen Parametern. Daher werden auch keine Daten über das Fahrzeug, dessen Fahrer oder dessen Halter erhoben, mit einem Fahndungsbestand abgeglichen oder gar gespeichert und weiterverarbeitet. Im Rahmen einer solchen Fahrzeugzählung kommt es lediglich darauf an, wie viele Fahrzeuge – ggf. mit einem bestimmten Kennzeichenfragment – die Kontrollstelle passieren. Persönliche Daten spielen in diesem Zusammenhang keine Rolle. Diese Maßnahme ist faktisch nichts anderes, als wenn Polizeibeamte auf einer Brücke postiert werden und eine Strichliste über die Anzahl der vorbeifahrenden Fahrzeuge erstellen oder bei jedem Fahrzeug auf eine Zähluhr drücken. Durch den Einsatz der Technik wird diese Fahrzeugzählung lediglich effektiviert und präzisiert. Zudem werden personelle Ressourcen eingespart, die an anderer Stelle zum Einsatz kommen können. Mangels Erhebung personenbezogener Daten findet ein Eingriff in das Recht auf informationelle Selbstbestimmung dabei nicht statt. Für diese Maßnahme bedarf es daher keiner speziellen Ermächtigungsgrundlage.

Zusammenfassend lässt sich festhalten, dass ein Eingriff in das Recht auf informationelle Selbstbestimmung nicht anzunehmen ist, sofern ausschließlich eine Kennzeichenzählung vorliegt oder die passierenden Fahrzeuge zwar erfasst, die erhobenen Daten aber unverzüglich mit dem Fahndungsbestand abgeglichen und anschließend sofort gelöscht werden, ohne dass eine weitergehende Auswertung erfolgt oder ein Personenbezug hergestellt werden kann.[244] Werden die erfassten Daten hingegen gespeichert, sodass sie ausgewertet und zur Grundlage von Anschlussmaßnahmen gemacht werden können, liegt ein Eingriff in das Recht auf informationelle Selbstbestimmung vor.[245]

---

242 So auch BVerfG, 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008, Abs. 69, 73.

243 Siehe oben Teil A, Pkt. 2.3.

244 Vgl. BVerfG, 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008, Abs. 68.

245 Vgl. BVerfG, 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008, Abs. 62 ff.

### *3.3 Rechtfertigung der Eingriffe*

Das Recht auf informationelle Selbstbestimmung ist nicht schrankenlos gewährleistet. In vielen Fällen benötigt die Polizei personenbezogene Daten, um Gefahren effektiv abwehren oder begangene Straftaten aufklären zu können.[246] Wie das Bundesverfassungsgericht schon in seinem Volkszählungsurteil feststellt, ist das Recht auf informationelle Selbstbestimmung daher nicht als absolute, uneinschränkbare Herrschaft des Einzelnen über die eigenen Daten zu verstehen.[247] Vielmehr muss der Einzelne als gemeinschaftsbezogene und gemeinschaftsgebundene Persönlichkeit[248] hoheitliche Eingriffe in sein Recht auf informationelle Selbstbestimmung hinnehmen, sofern das Allgemeininteresse überwiegt, der jeweilige Eingriff auf einer verfassungsgemäßen Ermächtigungsgrundlage beruht und die Maßnahme auch im Einzelfall verhältnismäßig ist.[249]

Die vom Bundesverfassungsgericht vorgegebenen Anforderungen an grundrechtsbeschränkende Ermächtigungsgrundlagen sind recht hoch. Insbesondere setzt eine Rechtfertigung der stattfindenden Eingriffe voraus, dass die jeweils einschlägige Ermächtigungsgrundlage Normenklarheit aufweist und hinreichend bestimmt ist.[250] Anlass, Zweck und Grenzen der Maßnahme müssen also präzise und bereichsspezifisch festgelegt werden.[251] Auf diese Weise soll sichergestellt werden, dass der demokratisch legitimierte Gesetzgeber bei Grundrechtseingriffen alle wesentlichen Entscheidungen selbst trifft, den Exekutivorganen für die jeweilige Maßnahme „steuernde und begrenzende Handlungsmaßstäbe" bereitgestellt werden und die Judikative eine wirksame Rechtskontrolle durchführen kann.[252] Sofern es – wie im vorliegenden Fall – um einen Eingriff in das Recht auf informationelle Selbstbestimmung geht, hat das Bestimmtheitsgebot zudem die Funktion, den Anlass der Maßnahme einerseits sowie die Verwendungsmöglichkeiten der erhobenen Informationen andererseits zu begrenzen.[253] Es muss dem Einzelnen möglich sein, zu wissen, „wer was wann und bei welcher Gelegenheit" über ihn weiß.[254] Welche Anforderungen das Bestimmtheitsgebot an die jeweilige Norm konkret stellt, hängt von der geregelten Maßnahme und deren Eingriffsschwere im Einzelfall ab.[255]

---

246 OLG Düsseldorf, JR 1999, 255, 256; *Burghard*, Kriminalistik 1994, 227; *Mauz/Dürig-Di Fabio*, Art. 2 Rn. 179.

247 BVerfGE 65, 1, 43 f.

248 Vgl. BVerfGE 4, 7, 15 f.; 8, 274, 329; 56, 37, 49; 65, 1, 43 f.

249 Vgl. BVerfGE 65, 1, 43 f.; *Robrecht*, NJ 2008, 9, 10; *Arzt*, SVR 2004, 321, 323; *Mauz/Dürig-Di Fabio*, Art. 2 Abs. 179.

250 BVerfGE 65, 1, 43; BVerfG 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008, Abs. 75, 93 ff.

251 BVerfGE 100, 313, 359 f; 110, 33, 53; BVerfG 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008, Abs. 94.

252 BVerfG 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008, Abs. 94; BVerfGE 110, 33, 53 f.

253 BVerfGE 65, 1, 46; 113, 348, 376; BVerfG 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008, Abs. 96; vgl. zum Zweckbindungsgebot ferner BVerfGE NJW 2007, 2464, 2466 f.

254 BVerfGE 65, 1, 43.

255 BVerfG 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008, Abs. 76.

Im Hinblick auf die automatische Kennzeichenfahndung ist besonders umstritten, welche Anforderungen an die Beschreibung des Fahndungsbestandes, mit dem die erfassten Kennzeichen abgeglichen werden, zu stellen sind. Die hessische Landesregierung sowie der Landtag und die Landesregierung von Schleswig-Holstein haben vor dem Bundesverfassungsgericht vorgetragen, der Begriff des Fahndungsbestandes als solcher sei hinreichend konkret und müsse nicht näher definiert werden.[256] Er erfasse all diejenigen Fahndungsdateien, auf die die Polizeibehörden im Rahmen ihrer Tätigkeit zur Suche nach Personen oder Sachen zugreifen dürfen. Als einschlägige Dateien wurden die Verbunddateien „Sachfahndung" und die Sachfahndung nach dem Nationalen Schengener Informationssystem (NSIS) des polizeilichen Informationssystems INPOL genannt. Andere Dateien seien von dem Begriff des Fahndungsbestandes nicht erfasst und ein Abgleich mit ihnen daher rechtswidrig.[257] Zudem wurde darauf verwiesen, dass der Begriff des Fahndungsbestandes auch in anderen Normen des Landes- und Bundesrechts verwendet werde und dort bislang nicht als zu unbestimmt gerügt worden sei.[258]

Kritiker tragen hingegen vor, dem Begriff des Fahndungsbestandes sei weder zu entnehmen welche, noch wie viele Daten in der Abgleichsdatei enthalten sein dürfen. Es müsse explizit festgelegt werden, dass nur solche Daten in die Abgleichsdatei aufgenommen werden, die zu dem angestrebten (präventiven oder repressiven) Zweck gespeichert wurden. Ein nicht weiter definierter Verweis auf den Fahndungsbestand als solchen sei nicht hinreichend bestimmt. [259]

Ob der Fahndungsbestand tatsächlich näher beschrieben werden muss, lässt das Bundesverfassungsgericht in seinem Urteil vom 11. März 2008 offen. Es weist lediglich darauf hin, dass es bislang an einer allgemein anerkannten Definition des „Fahndungsbestandes" fehlt[260] und der Begriff daher nicht dazu geeignet ist, einen nicht hinreichend bestimmten Anlass oder Zweck der Maßnahme einzugrenzen. Hingegen kann sich in diesen Fällen schon aus dem Zweck der Maßnahme ergeben, welche Daten in den Fahndungsbestand aufgenommen werden dürfen. Dies ist in § 36a BbgPolG gegeben. Die Erstellung der Suchdateien unterliegt gemäß Abs. 2 genau der Zweckbestimmung des Abs. 1. Die Gesetzeslage in Brandenburg unterscheidet sich schon an dieser Stelle grundlegend von den 2008 vom BVerfG gerügten Regelungen.

Um den Anforderungen an eine verfassungskonforme Regelung zu genügen, müssen sowohl die grundrechtsbeschränkende Ermächtigungsgrundlage als auch die darauf gestützte Einzelmaßnahme verhältnismäßig sein. Eine Ermächtigungsgrundlage und eine hoheitliche Maß-

---

256 Siehe BVerfG 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008, Abs. 43, 53. So auch *Lang*, JurPC Web-Dok. 93/2005, Abs. 84.

257 Hessische Landesregierung, BVerfG 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008, Abs. 43.

258 Landtag und Landesregierung von Schleswig-Holstein, BVerfG, 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008, Abs. 53.

259 Siehe BVerfG, 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2010, Abs. 33.

260 Siehe v.a. BVerfG 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008, Abs. 100, 107 ff., 130.

nahme sind immer dann verhältnismäßig, wenn sie einen legitimen Zweck verfolgen und das eingesetzte Mittel zur Erreichung dieses Zwecks geeignet, erforderlich und angemessen ist.[261] Die Kennzeichenfahndung wird sowohl zur Gefahrenabwehr als auch zur Strafverfolgung eingesetzt. Beide Aufgabenbereiche dienen dem Schutz von besonders wichtigen Rechtsgütern.[262] Eine polizeiliche Maßnahme ist zur Erfüllung des angestrebten Zwecks geeignet, sofern sie dessen Erreichung ermöglicht, fördert oder auch nur erleichtert.[263] Erforderlich ist sie immer dann, wenn sich der angestrebte Erfolg nicht ebenso effektiv durch ein anderes, milderes Mittel erreichen lässt.[264] Ob die automatische Kennzeichenfahndung ein zur Erfüllung des jeweils angestrebten Zwecks geeignetes und erforderliches Mittel darstellt, muss für jeden Einsatzbereich gesondert geprüft werden.

Angemessen ist eine Maßnahme nach ständiger Rechtsprechung immer dann, wenn der Eingriff in das betroffene Grundrecht nicht außer Verhältnis zu dem verfolgten Zweck steht.[265] Insbesondere darf der Grundrechtseingriff nicht weitergehen, als dies zum Schutz der öffentlichen Interessen unerlässlich ist.[266] Zudem ist von Bedeutung, welche Persönlichkeitsrelevanz die von der Maßnahme betroffenen Informationen haben, sowie jene Informationen, die aus der Maßnahme mittels Weiterverarbeitung und Verknüpfung gewonnen werden.[267] Je weiter die Daten in den privaten Lebensbereich des Betroffenen hineinreichen, desto höher sind die Anforderungen an den verfolgten Zweck und die einschlägige Ermächtigungsgrundlage.[268]

Des Weiteren wird die Schwere des Grundrechtseingriffs davon beeinflusst, ob die Maßnahme offen oder verdeckt durchgeführt wird. Von einer verdeckten Maßnahme wird nach Angaben der Polizei nur dann gesprochen, wenn die zuständige Behörde die Durchführung der Maßnahme bewusst verschleiert und für den Betroffenen unkenntlich macht.[269] Ist dem Betroffenen schlichtweg nicht bekannt, dass die Maßnahme durchgeführt wird, erkennt er sie erst im letzten Moment, sodass er sich der Maßnahme nicht entziehen kann, oder ist sie für ihn mangels Sachkenntnis nicht definierbar (z. B. weil er nicht weiß, wie die entsprechende Technik aussieht oder welchem Zweck die aufgebauten Kameras dienen), handelt es sich nicht allein deshalb um eine verdeckte oder auch „heimliche" Maßnahme.[270] Sofern eine

---

261 BVerfGE 109, 279, 335; BVerfG 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008, Abs. 163.

262 BVerfG 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008, Abs. 164.

263 BVerfG 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008, Abs. 165.

264 BVerfGE 115, 320, 345; *Roßnagel*, DAR 2008, 61, 64.

265 Vgl. BVerfGE 109, 279, 349 f.; BVerfG 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008, Abs. 168; *Würtenberger/Heckmann*, Rn. 530.

266 BVerfGE 65, 1, 46; *Maunz/Dürig-Di Fabio*, Art. 2 Abs. 181.

267 BVerfG 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008, Abs. 77, 80; *Frenz*, DVBl. 2009, 333, 337.

268 Vgl. BVerfG, 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008, Abs. 76.

269 Vgl. bspw. Art. 30 Abs. 3 BayPAG.

270 Vgl. BVerfG 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008, Abs. 79, 89; *Roßnagel*, NJW 2008, 2547.

Maßnahme in verdeckter Form durchgeführt wird, ist es dem Betroffenen nicht möglich, vorherigen Rechtsschutz einzuholen. Auch die Einholung nachträglichen Rechtsschutzes kann erschwert oder gar unmöglich sein. Aus diesem Grund wiegt der stattfindende Grundrechtseingriff bei einer heimlichen Überwachungsmaßnahme deutlich schwerer, als wenn dieselbe Maßnahme offen erfolgt.[271]

Schließlich ist noch zu berücksichtigen, dass Kennzeichenfahndung ausschließlich auf öffentlichen Straßen und Plätzen eingesetzt wird. Sowohl das Bewegungsverhalten des betroffenen Bürgers als auch das erfasste Kennzeichen sind allgemein ersichtlich und für jedermann erkennbar. Die zuständige Stelle verschafft sich also nicht Zugang zu „verdeckten" Daten, sondern greift lediglich auf allgemein zugängliche Informationen zu. Zudem liegt der Sinn und Zweck eines Kfz-Kennzeichens gerade darin, eine Identifizierung des Fahrzeuges, des Halters und auch des Fahrers zu ermöglichen. Dadurch werden die stattfindenden Grundrechtseingriffe zwar nicht beseitigt, in ihrem Gewicht aber deutlich reduziert.[272]

Eine verfassungskonforme Ermächtigungsgrundlage muss in abstrakter Form unter Berücksichtigung aller Aspekte einen Ausgleich zwischen den Grundrechten des Bürgers und der Schutzpflicht des Staates schaffen,[273] der sich dann in der konkreten Maßnahme fortsetzen kann. Die Anforderungen an die Verhältnismäßigkeit werden dabei von der Art und Intensität des Grundrechtseingriffs determiniert.[274] Wie schwer der Grundrechtseingriff tatsächlich wiegt, wird einerseits von der Bedeutung des betroffenen Grundrechts, andererseits aber auch von der Bedeutung des gefährdeten oder verletzten Rechtsguts, der Nähe der Gefahr und der Wahrscheinlichkeit ihrer Verwirklichung beeinflusst.[275] Um den Einsatz sachgerecht bewerten zu können, ist es daher erforderlich, dessen konkreten Zweck im Einzelfall zu überprüfen.

In Brandenburg wird die automatische Kennzeichenfahndung sowohl präventiv als auch repressiv eingesetzt. Zulässig ist sie nur bei einem konkreten Anlass. Ein allgemeiner, anlassunabhängiger Abgleich mit INPOL-,[276] Schengen-[277] und anderen allgemeinen Fahndungsbeständen[278] ist ausdrücklich nicht zulässig.[279]

---

271 BVerfG 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008, Abs. 79, 89; Braun/Seidl, jurisPR-ITR 13/2010 Anm. 6.

272 BVerfG 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008, Abs. 83.

273 BVerfGE 109, 279, 350; BVerfG 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008, Abs. 168.

274 BVerfG 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008, Abs. 75 f.

275 Vgl. auch BVerfG 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008, Abs. 76.

276 Bei INPOL handelt es sich um eine länderübergreifende Datenbank, welche teilweise als INPOL-zentral vom BKA und teilweise als INPOL-Land von den Ländern geführt wird. INPOL setzt sich aus verschiedenen Dateien zusammen. Zu den wichtigsten zählen der Kriminalaktennachweis (KAN), die Personen- und Sachfahndung, die Haftdatei, der Erkennungsdienst sowie die DNA-Analyse-Datei. Neben dem BKA und den Landeskriminalämtern sind auch die Polizeibehörden der Länder, die Bundespolizei und bestimmte Behörden des Zolls dazu berechtigt, Daten in das System einzugeben oder aus selbigem abzurufen. Siehe dazu auch *Graf*, S. 157, Fn. 581.

277 Das Schengener Informationssystem (SIS) ist eine länderübergreifende Datenbank. Sie enthält Informationen über Personen nach denen gefahndet wird, die zur nationalen Einreiseverweigerung

Zur Gefahrenabwehr ist die Maßnahme auf der Grundlage von § 36a Abs. 1 BbgPolG möglich:

- zur Abwehr einer gegenwärtigen Gefahr für Leib oder Leben (Nr. 1),
- zur Abwehr einer gegenwärtigen Gefahr, wenn die Voraussetzungen für eine Identitätsfeststellung nach § 12 Abs. 1 Nr. 2 bis 4 BbgPolG erfüllt sind (d.h. an gefährlichen Orten, an gefährdeten Objekten und an Kontrollstellen vor Veranstaltungen) (Nr. 2) sowie
- zur Fahndung nach Personen und Fahrzeugen, die zur polizeilichen Beobachtung ausgeschrieben wurden (Nr. 3).

Zur Strafverfolgung kann die Maßnahme ferner eingesetzt werden:

- zur Eilfahndung nach bekannten Kfz-Kennzeichen zur Verfolgung von Straftaten von erheblicher Bedeutung gemäß § 100h Abs. 1 Nr. 2 StPO,
- zur längerfristigen Observation gemäß §§ 100h Abs. 1 Nr. 2 i.V.m. 163f Abs. 1 Nr. 2 u. Abs. 3 StPO,
- zur Ringalarmfahndung gem. § 111 StPO sowie
- zur polizeilichen Beobachtung gem. § 186e StPO bei Straftaten von erheblicher Bedeutung.

Auch im Fall der Einsätze auf der Grundlage der verschiedenen strafprozessualen Rechtsgrundlagen kommen als Fahndungsgrundlage nur die auf der Basis des § 36a Abs. 2 BbgPolG erstellten Suchdateien zur Anwendung. Dies wird durch die Rahmenrichtlinie zur automatischen Kennzeichenfahndung klargestellt.[280]

In der Praxis wird sie derzeit vorwiegend zur gezielten Suche nach bereits bekannten Kfz-Kennzeichen eingesetzt.[281] An erster Stelle steht dabei die Fahndung nach gestohlenen Fahrzeugen, gefolgt von der Fahndung nach Gewalttätern, die eine bestimmte Veranstaltung aufsuchen wollen. Ob und unter welchen Voraussetzungen die dabei stattfindenden Eingriffe gerechtfertigt sind, soll nun für jeden Einsatzzweck gesondert geprüft werden. Mit Ausnahme der Kfz-Diebstähle, die eine besondere Fallkonstellation mit repressiven und präventiven Aspekten darstellen und den Hauptanteil der Einsätze ausmachen, soll eine Prüfung der repressiv fundierten Maßnahmen nach der StPO an dieser Stelle unterbleiben, da dies nicht von dem Untersuchungsauftrag gedeckt wäre.

---

ausgeschrieben sind sowie Daten über vermisste Personen. Ferner werden im SIS auch Fahrzeuge und andere Sachen geführt, nach denen bspw. zwecks Sicherstellung oder Beweissicherung gesucht wird. Zugriff auf diese Daten haben lediglich die in Art. 101 SDÜ genannten Stellen der Mitgliedsstaaten. Für Einzelheiten siehe Titel IV SDÜ.

278 Dazu *Zöller*, NVwZ 2005, 1235 f.; *Arzt*, SVR 2004, 321, 324.

279 Rahmenrichtlinie zur automatischen Kennzeichenfahndung in der Polizei Brandenburg vom 23.12.2009.

280 Siehe Fn. 279.

281 Siehe unten Teil E, Pkt. 3.

### *3.3.1 Gegenwärtige Gefahr für Leib oder Leben (§ 36a Abs. 1 Nr. 1 BbgPolG)*

Die Abwehr von gegenwärtigen Gefahren für Leib oder Leben von Menschen betrifft die höchsten von der Verfassung geschützten Werte (siehe Art. 2 Abs. 2 GG). Ihr Schutz kann selbst erhebliche Grundrechtseingriffe rechtfertigen. Er zählt zu den Grundaufgaben der Polizei. Nähere Ausführungen zu diesem Einsatzzweck erübrigen sich an dieser Stelle.

### *3.3.2 Suche nach gestohlenen Kraftfahrzeugen*

Die automatische Kennzeichenfahndung wird nicht nur in Brandenburg, sondern auch in anderen Bundesländern[282] wie auch im Ausland primär im Kampf gegen die Kfz-Kriminalität eingesetzt.[283] Zu prüfen ist, ob Kfz-Diebstahl eine Straftat von erheblicher Bedeutung ist. Nach etwa 15 Jahren des Rückgangs von Kfz-Diebstählen steigt ihre Zahl deutschlandweit seit dem Jahr 2009 erstmals wieder an. Etwa 40.000 kaskoversicherte Kraftfahrzeuge wurden 2009 in Deutschland entwendet, die meisten davon in Berlin (siehe Übersicht 4). In Brandenburg steigen die Zahlen sogar schon seit einigen Jahren deutlich an. Das Land hatte 2009 nach Berlin die zweithöchste Häufigkeitszahl. Sie liegt mit einem Wert von 131 Entwendungen pro 100.000 Einwohner fast zweieinhalb Mal so hoch wie im Bundesdurchschnitt. Der von den Versicherungen erstattete Schaden belief sich 2009 deutschlandweit auf ca. 218 Mio. Euro.[284]

*Übersicht 4: Kfz-Diebstahl in Deutschland gemäß Polizeilicher Kriminalstatistik**

**Häufigkeitszahlen in den Ländern**
Diebstahl insgesamt von Kraftwagen einschl. Gebrauchsentwendung (***100)
*T154*

| Land | erfasste Fälle insgesamt | AQ in % | Häufigkeitszahl*) 2009 | 2008 | 2007 | 2006 | 2005 | 2004 | 2003 |
|---|---|---|---|---|---|---|---|---|---|
| Baden-Württemberg | 1 517 | 36,6 | 14 | 15 | 20 | 24 | 25 | 31 | 34 |
| Bayern | 2 610 | 60,0 | 21 | 20 | 20 | 21 | 23 | 27 | 28 |
| Berlin | 7 262 | 9,0 | 212 | 154 | 150 | 160 | 180 | 210 | 261 |
| Brandenburg | 3 317 | 26,2 | 131 | 112 | 97 | 96 | 112 | 168 | 189 |
| Bremen | 434 | 25,3 | 66 | 63 | 88 | 98 | 140 | 197 | 219 |
| Hamburg | 2 041 | 10,5 | 115 | 116 | 116 | 134 | 154 | 239 | 289 |
| Hessen | 1 728 | 38,1 | 28 | 29 | 40 | 50 | 72 | 89 | 86 |
| Mecklenburg-Vorpommern | 985 | 34,2 | 59 | 60 | 96 | 90 | 116 | 180 | 219 |
| Niedersachsen | 3 422 | 29,8 | 43 | 39 | 42 | 44 | 54 | 64 | 66 |
| Nordrhein-Westfalen | 7 570 | 28,5 | 42 | 45 | 48 | 52 | 63 | 72 | 81 |
| Rheinland-Pfalz | 1 319 | 50,0 | 33 | 33 | 36 | 40 | 46 | 46 | 53 |
| Saarland | 410 | 34,6 | 40 | 52 | 55 | 53 | 58 | 65 | 63 |
| Sachsen | 3 862 | 19,5 | 92 | 69 | 52 | 50 | 61 | 82 | 89 |
| Sachsen-Anhalt | 1 782 | 28,1 | 75 | 71 | 77 | 71 | 87 | 112 | 132 |
| Schleswig-Holstein | 1 418 | 23,5 | 50 | 40 | 53 | 58 | 62 | 86 | 91 |
| Thüringen | 698 | 34,0 | 31 | 34 | 38 | 39 | 44 | 69 | 71 |
| Bundesgebiet insgesamt | 40 375 | 26,7 | 49 | 45 | 48 | 51 | 61 | 77 | 86 |

*) Quelle: BKA, Polizeiliche Kriminalstatistik 2009, S. 177.

---

282 Siehe oben Teil B, Pkt. 2

283 Siehe oben Teil C.

284 Angaben des Gesamtverbandes der Deutschen Versicherungswirtschaft e.V.

Sobald ein Kfz-Diebstahl zur Anzeige gebracht wird, kann die Polizei das entsprechende Kennzeichen in den Fahndungsbestand aufnehmen und eine automatische Kennzeichenfahndung einleiten. Auf diese Weise soll das Fahrzeug möglichst rasch lokalisiert, eine Verschiebung ins Ausland verhindert und eine Ergreifung der Täter ermöglicht werden. Die automatische Kennzeichenfahndung dient in diesen Fällen also zunächst den gefahrenabwehrrechtlichen Zielen, einen endgültigen Eigentumsverlust zu verhindern und die rechtmäßige Besitzlage wiederherzustellen. Diese Materie muss mangels abweichender Zuweisungsnorm gem. Art. 30, 70 GG von den Bundesländern geregelt werden. Davon hat Brandenburg bislang keinen Gebrauch gemacht, sondern führt die Maßnahmen ausschließlich auf der Grundlage von § 100h Abs. 1 Nr. 2 StPO durch. Formale Zweckbestimmung ist daher die Aufklärung der Kfz-Diebstähle sowie die Festnahme des Täters oder der Tätergruppe.

Sowohl im präventiven als auch im repressiven Einsatzbereich handelt es sich bei allen genannten Zielen um verfassungslegitime Ziele von hohem Gewicht.[285] Dass die automatische Kennzeichenfahndung zur Erreichung der angestrebten Ziele prinzipiell geeignet ist, ergibt sich aus dem engen sachlichen Zusammenhang zu der Deliktsart. Eine zielführende Fahndung muss sich auf den Straßenraum konzentrieren, da die gesuchten Fahrzeuge dort bewegt werden. Das amtliche Kennzeichen, an dem sich die Fahndung orientiert, ist dabei das entscheidende Identifikationsmerkmal. Es ist kein anderes Mittel ersichtlich, welches die automatische Kennzeichenfahndung mit gleicher Effektivität ersetzen könnte, sodass die Maßnahme auch erforderlich ist.[286] Angemessen ist eine Maßnahme nach ständiger Rechtsprechung immer dann, wenn der Eingriff in das betroffene Grundrecht nicht außer Verhältnis zu dem verfolgten Zweck steht. Wird mit Hilfe der automatischen Kennzeichenfahndung nach entwendeten Fahrzeugen gesucht, beschränkt sich die Maßnahme eben auf die Fahndung nach diesen genau bestimmten, jeweils aktuell in den Fahndungsbestand eingestellten Kennzeichen. Zu berücksichtigen ist ferner, dass den Betroffenen durch ihr deliktisches Vorverhalten gegenüber dem rechtmäßigen Eigentümer auch den Anlass für die Maßnahme selbst gesetzt haben.[287] Die Kennzeichenfahndung ist darüber hinaus in Fällen der organisierten, grenzüberschreitenden Kfz-Kriminalität aufgrund der geographischen Lage Brandenburgs die einzige und zugleich letztmögliche Gelegenheit, ein Kfz gerade noch rechtzeitig vor der Überführung in das Ausland zu entdecken. Da die gesuchten Fahrzeuge mit Hilfe der automatischen Kennzeichenfahndung lediglich lokalisiert werden, handelt es sich im Übrigen um eine reine Hilfsmaßnahme, deren Eingriffsqualität *per se* eher im unteren Bereich anzusiedeln ist.[288] Alle weitergehenden Maßnahmen sind nicht Bestandteil der automatischen Kennzeichenfahndung, sondern Anschlussmaßnahmen, die einer eigenen Ermächtigungsgrundlage bedürfen.

---

285 Vgl. BVerfG 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008, Abs. 174.

286 So auch *Bodenbenner/Heinemann*, NVwZ 2010, 679, 681 und *Roßnagel*, DAR 2008, 61, 64.

287 Vgl. BVerfG 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008, Abs. 78.

288 Vgl. BVerfG 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008, Abs. 84.

Die Eingriffsintensität wird ferner dadurch limitiert, dass die Maßnahmen gem. § 100h Abs. 1 Nr. 1 StPO in Brandenburg auf 24 Stunden begrenzt sind.[289] Diese Limitierung ergibt sich weder aus dem brandenburgischen Polizeigesetz noch aus § 100h StPO, sondern ist eine Konsequenz aus der Abgrenzung der Eilfahndung zur längerfristigen Observation, die gem. § 163f Abs. 1 Nr. 1 StPO definiert ist als Beobachtung, die durchgehend länger als 24 Stunden dauert. Im Hinblick auf die Zielgenauigkeit, die faktisch ausschließt, dass Nichtbetroffene von der Maßnahme nicht tangiert werden, erscheint eine moderate Verlängerung vorstellbar. Dies könnte jedenfalls auf polizeirechtlicher Basis erfolgen.

Insgesamt handelt es sich mithin um ein angemessenes Mittel im Kampf gegen die oft grenzüberschreitende Kfz-Kriminalität. Insbesondere die hohen Schäden, die sowohl die individuellen Fahrzeughalter als auch deren Versicherung bei einem Kfz-Diebstahl regelmäßig erleiden, sowie die Bedeutung des Kfz-Diebstahls als flächendeckendes Kriminalitätsproblem rechtfertigen den Einsatz der automatischen Kennzeichenfahndung als gezielte und insgesamt wenig einschneidende Maßnahme[290] zur Verhütung, Verfolgung und Aufklärung von Kfz-Diebstählen.

### 3.3.3. *Abwehr einer gegenwärtigen Gefahr vor Veranstaltungen (§ 36a Abs. 1 Nr. 2 BbgPolG)*

Von gesteigerter Persönlichkeitsrelevanz ist die automatische Kennzeichenfahndung demgegenüber, wenn sie vor Veranstaltungen auf den entsprechenden Zufahrtsstraßen oder an dem Veranstaltungsort selbst zur gezielten Suche nach potentiellen Störern oder Straftätern eingesetzt wird. In diesem Fall begrenzt sich der Ertrag der Maßnahme nicht auf die Tatsache, dass das Fahrzeug mit dem entsprechenden amtlichen Kennzeichen an dem bestimmten Tag zur gewissen Uhrzeit auf der überwachten Straße in eine bestimmte Fahrtrichtung unterwegs war, sondern sie gibt auch Aufschluss darüber, dass der Fahrer des gesuchten Fahrzeuges wahrscheinlich eine bestimmte Veranstaltung besuchen wollte.

Die Maßnahme ist zulässig, wenn die Voraussetzungen einer Identitätsfeststellung nach § 12 Abs. 1 Nr. 2 bis 4 BbgPolG vorliegen. Dies betrifft Maßnahmen an gefährlichen Orten, z.B. bekannte Rockertreffpunkte oder Treffpunkte von Fußballfans einschließlich möglicher Orte, wo rivalisierende Gruppen der konkurrierenden Vereine aufeinandertreffen könnten, ferner Maßnahmen an gefährdeten Orten, z.B. potenzielle Ziele terroristischer Anschläge, sowie Kontrollstellen auf Anreisewegen zu Veranstaltungen.

Eine Rechtfertigung der stattfindenden Eingriffe unterliegt daher höheren Anforderungen, als es bei der Fahndung nach gestohlenen Kraftfahrzeugen der Fall ist. Dem wird jedenfalls dann entsprochen, wenn mit Hilfe der automatischen Kennzeichenfahndung nach Personen gesucht wird, bei denen aufgrund kriminalistischer Erfahrung davon auszugehen ist, dass sie andere

---

289 Rahmenrichtlinie zur automatischen Kennzeichenfahndung in der Polizei Brandenburg vom 23.12.2009.

290 Vgl. BVerfG 1 BvR 2074/05 und 1 BvR 1254/07 vom 11.03.2008, Abs. 82.

Personen in nicht unerheblichem Maß körperlich verletzen oder gar töten wollen. Zu Strafverfolgungszwecken ist der Einsatz der automatischen Kennzeichenfahndung vor Veranstaltungen dann verhältnismäßig, wenn die Maßnahme der Aufklärung besonders schwerer Straftaten dient. Zu denken ist dabei insbesondere an Straftaten nach §§ 89a, 129a, auch in Verbindung mit §§ 129 b Abs. 1, 250 Abs. 1 Nr. 1 StGB und die darin genannten Straftaten. Dies ist aufgrund langer kriminalistischer Erfahrung bei Personen, die zu der Gruppe der Gewalttäter Sport gehören, ebenso anzunehmen wie bei Mitgliedern der verschiedenen im Land aktiven Rockergruppen. Das gilt jedenfalls unter den Bedingungen der anlassbezogenen Kennzeichenfahndung in Brandenburg, wo nicht pauschal und ungeprüft die entsprechenden Dateien des BKA oder anderer Behörden – die nur bedingten Landesbezug aufweisen – zum Einsatz kommen, sondern wo ad hoc individuelle Fahndungsdateien generiert werden, die dann jeweils den aktuellen Stand der Erkenntnisse der brandenburgischen Polizeibehörden berücksichtigen und auf dieser Basis den aktuell verdächtigen Personenkreis – und nur diesen – umfassen.

### *3.3.4 Fahndung nach Personen oder Fahrzeugen, die zur polizeilichen Beobachtung ausgeschrieben wurden (§ 36a Abs. 1 Nr. 3 BbgPolG)*

Hierbei handelt es sich um eine eng begrenzte polizeiliche Sondersituation zur Verhinderung unmittelbar bevorstehender Straftaten, beipielsweise im Rahmen der Terrorismusbekämpfung. Die Maßnahme richtet sich gegen individuelle Personen und ergänzt lediglich die ohnehin zulässigen polizeilichen Maßnahmen um eine weitere technische Komponente. Ein zusätzlicher Grundrechtseingriff wird daraus nicht ersichtlich.

### *3.3.5. Weitere Einsatzvarianten, die in Brandenburg nicht zum Einsatz kommen*

Die automatische Kennzeichenerfassung ermöglicht zahlreiche weitere Anwendungsvarianten. Einige dieser Einsatzformen, die in den Nachbarländern praktiziert werden[291], sollen hier ergänzend aufgelistet werden. Hiervon würden einzelne nach deutscher Rechtsauffassung sicherlich problematisch erscheinen. Der Vergleich vermag aufzuzeigen, dass sich der Gesetzgeber in Brandenburg bei der Entscheidung über die zuzulassenden Alternativen sehr bewusst Grenzen gesetzt und den Einsatzbereich der Maßnahmen auf solche Konstellationen beschränkt hat, die bei einer verfassungsrechtlichen Bewertung Bestand haben können. Solche weiterreichenden Einsatzformen aus der ausländischen Praxis sind insbesondere:

- der anlassunabhängige Abgleich mit dauerhaft eingespeisten Dateien, insbes. dem allgemeinen Fahndungsbestand (insbesondere unter Heranziehung der INPOL- und SIS-Bestände),
- die Fahndung nach „Versicherungssündern“,
- die Verfolgung „unnötigen Herumfahrens",
- die Parkplatzüberwachung auf großen Transitrouten; sie soll vor allem der Bekämpfung des LKW-/Warendiebstahls und der Drogenkriminalität dienen,

---

291 Siehe ausführlich oben Teil C.

- die mobile Überwachung des ruhenden Verkehrs auf der Suche nach Bußgeldsündern,
- die Aufzeichnung von Kennzeichen als technische Grundlage für neuartige Geschwindigkeitskontrollsysteme[292].

Die aufgeführten Varianten kommen insbesondere in den Niederlanden und der Schweiz zur Anwendung.

[292] Hierzu werden bspw. die Kennzeichen aller Fahrzeuge, die eine bestimmte Tunnelein- und Ausfahrt passieren, registriert und aus der Durchlaufzeit die Durchschnittsgeschwindigkeit errechnet.

# Teil E: Anwendungspraxis

## 1. Einleitung

Ein Hauptziel der Evaluation besteht neben der Prüfung des rechtlichen Rahmens der untersuchungsgegenständlichen Maßnahmen in einer kritischen Bestandsaufnahme der gegenwärtigen Anwendungspraxis. Hierfür wurden alle verfügbaren Daten und weiterführenden Informationen zusammengetragen und analysiert, um auf dieser Basis ein möglichst realistisches Abbild der Praxis zu gewinnen.

Soweit möglich wurden neben aggregierten Datenbeständen (Statistiken, Einträge aus dem elektronischen Einsatzleit- und Erfassungssystem ELBOS) auch individuelle Fallakten und -aufzeichnungen ausgewertet. Dies betraf insbesondere richterliche Beschlüsse im Rahmen der Abfrage von Telekommunikations-Verkehrsdaten. Insgesamt ist der Umfang solcher polizeilicher Aufzeichnungen freilich begrenzt und weist bei Weitem nicht die Informationsdichte auf, wie sie der Forschung regelmäßig bei strafverfahrensbezogenen Aktenauswertungen zur Verfügung steht. Zu vielen der in dem Untersuchungsschema ursprünglich vorgesehenen Variablen[293] konnte im Ergebnis leider keine hinreichende Datenbasis gewonnen werden, die eine seriöse Auswertung möglich gemacht hätte.

## 2. Verkehrsdatenabfrage und Ortung von Mobiltelefonen

### *2.1 Anzahl der Einsätze und Entwicklung der Einsatzzahlen*

Sämtliche Maßnahmen im Untersuchungszeitraum waren auf die Standortbestimmung ausgerichtet. Dies geschah in nahezu allen Fällen durch Abfrage der entsprechenden Geodaten bei den Telekommunikationsanbietern. Sowohl 2009 als auch 2010 gab es jeweils nur einen Einsatz, in dem die Mobilfunkortung auf der Basis des § 33b Abs. 3 Nr. 2 BbgPolG durch die Polizei selbst unter Verwendung des IMSI-Catchers durchgeführt wurde. Die genauen Einsatzzahlen ergeben sich aus Tabelle 1. Danach waren für 2009 insgesamt 161 Maßnahmen zu verzeichnen, im Jahr 2010 waren es 180.

*Tabelle 1: Häufigkeit der Verkehrsdatenabfrage und Mobilfunkortung*

| Einsatzart | 2009 | 2010* | Gesamt |
|---|---|---|---|
| § 33b VI 2 BbgPolG | 160 | 179 | 339 |
| § 33b III Nr. 2 BbgPolG | 1 | 1 | 2 |
| **insgesamt** | **161** | **180** | **341** |

*) Für 2010 vorläufige Zahlen des Ministeriums des Innern; der Evaluationszeitraum umfasste im Jahr 2010 lediglich die Monate Januar bis Juni; in diesen Zeitraum entfallen 98 Maßnahmen gem. § 33b VI 2 und keine nach § 33b III Nr. 2 BbgPolG.

293 Vgl. den Variablenplan in Teil G, Anlage 3. Merkmale, zu denen für eine ausreichende Anzahl von Fällen Informationen generiert werden konnten, sind dort grau unterlegt.

In dem einzigen Einsatzfall des IMSI-Catchers im Jahr 2009 war im Übrigen zunächst auch eine Abfrage gem. § 33b Abs. 6 S. 2 erfolgt, sodass beide Einsätze bei der weiteren Auswertung als ein Fall gezählt wurden. Auch im Übrigen erscheint eine gliederungstechnisch getrennte Behandlung der einen Maßnahme gem. § 33b Abs. 3 Nr. 2 BbgPolG nicht sinnvoll.

Nicht alle Fälle aus dem Jahr 2010 fallen in den Evaluationszeitraum. Dieser umfasst, wie in Teil A beschrieben, für die präventive Verkehrsdatenabfrage und Mobilfunkortung das gesamte Jahr 2009 sowie das erste Halbjahr 2010. Die in diesen Zeitraum fallende Grundgesamtheit von insgesamt 258 Einsätzen wurde im Rahmen der Auswertung näher analysiert und bildet die Datenbasis für die nachfolgenden Darstellungen. Die genauen Einsatzzahlen und die zeitliche Verteilung für den Evaluationszeitraum ergeben sich zunächst aus Tabelle 2, und zwar in monatlichen Intervallen.

*Tabelle 2: Einsatzzahlen im zeitlichen Verlauf (1.1.2009 bis 30.6.2010)*

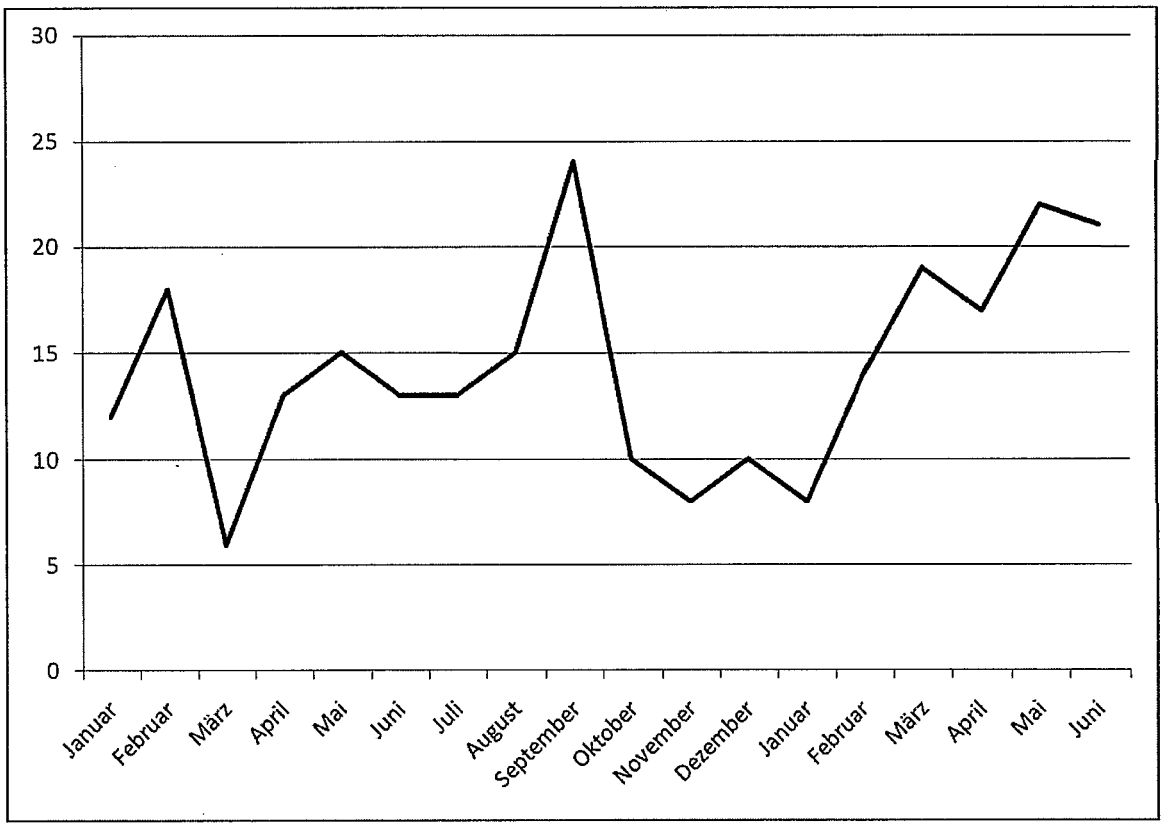
| Jahr | Monat | Maßnahmen |
|---|---|---|
| 2009 | Januar | 12 |
| 2009 | Februar | 18 |
| 2009 | März | 6 |
| 2009 | April | 13 |
| 2009 | Mai | 15 |
| 2009 | Juni | 13 |
| 2009 | Juli | 13 |
| 2009 | August | 15 |
| 2009 | September | 24 |
| 2009 | Oktober | 10 |
| 2009 | November | 8 |
| 2009 | Dezember | 10 |
| 2010 | Januar | 8 |
| 2010 | Februar | 14 |
| 2010 | März | 19 |
| 2010 | April | 17 |
| 2010 | Mai | 22 |
| 2010 | Juni | 21 |
| **insgesamt** | | **258** |

Es wird bereits aus dieser Grundverteilung deutlich, dass sich die Fälle recht gleichmäßig über die einzelnen Monate verteilen. Durchschnittlich waren 15 Anwendungsfälle pro Monat zu verzeichnen. Nennenswerte Abweichungen von mehr als 5 Punkten beschränken sich auf wenige Fälle, und zwar nach oben im September 2009 mit dem Spitzenwert von 24 Fällen und zuletzt knapp im Mai und Juni 2010, sowie gleichfalls dreimal nach unten, und zwar im März 2009 mit nur 6 sowie im November 2009 und im Januar 2010 mit jeweils 8 Maßnahmen.

Der beschriebene Verlauf wird in Schaubild 1 auch grafisch sehr gut sichtbar. Die Einsatzzahlen variieren unregelmäßig und bewegen sich in der Mehrzahl in dem Varianzintervall unter- und oberhalb des Durchschnittswertes (10 bis 20); einmal wird der Wert von 10 deut-

lich unterschritten. Dasselbe gilt, im gleichen Ausmaß, für den Ausschlag vom September 2009 nach oben; dieser einmalige Spitzenwert dominiert den Eindruck insgesamt. Über den gesamten Referenzzeitraum hinweg ist insgesamt weder eine kontinuierliche Abnahme noch eine entsprechende Zunahme der Maßnahmen zu erkennen. Lediglich für die letzten beiden Quartale deutet sich ein etwas stabilerer Trend nach oben an.

*Schaubild 1: Entwicklung der Einsatzzahlen absolut im zeitlichen Verlauf*




Dieser Trend stabilisiert sich bei Berücksichtigung des gesamten Fallaufkommens der Polizei. Hierbei handelt es sich bekanntlich nicht um eine feste Bezugsgröße. Polizeiliches Handeln ist in weitem Umfang reaktiv und wird durch die Nachfrage von Bürgerseite ausgelöst. Mit der schwankenden Nachfrage variiert auch das Aufkommen von Notrufen und Gefahrensituationen, die das Einsatzspektrum der Verkehrsdatenabfrage ausmachen (siehe unten 2.3). Aus diesem Grund müssen die Maßnahmen zwingend in Relation zu der jeweiligen Gesamtzahl aller polizeilichen Einsätze gesetzt werden. Als geeignete Vergleichsgröße wurden die Einsatzzahlen aus dem in Brandenburg implementierten elektronischen Einsatzleitsystem ELBOS herangezogen. Dabei handelt es sich um das Zentralsystem der Polizei des Landes Brandenburg zur Einsatzführung, Einsatzbearbeitung und Einsatzdokumentation in der Leitstelle und den Polizeiwachen. Jedem neuen Einsatz wird zentral und automatisch eine fortlaufende Kennzahl zugewiesen. Sie entspricht damit funktional weithin einer Tagebuchnummer im traditionellen Sinne. Auch wenn es sich bei ELBOS um kein amtliches Statistiksystem handelt, erlauben die Einsatzzahlen selbst unter der Einschränkung, dass grundsätzlich Sachverhalte und Maßnahmen denkbar sind, die außerhalb des Leitsystems erledigt werden,

Trendaussagen zu dem Umfang der polizeilichen Tätigkeit in Brandenburg. Mangels Verfügbarkeit anderer lückenloser Statistiken bieten sie jedenfalls für den vorliegenden Untersuchungszweck eine geeignete Vergleichsgrundlage.

Die von ELBOS registrierten Einsatzzahlen lassen sich differenzieren nach Maßnahmen zur Gefahrenabwehr, solchen zur Strafverfolgung, Verkehrsdelikte und Verkehrsunfälle, Maßnahmen zur Durchsetzung ziviler Rechtsansprüche sowie interne Maßnahmen ohne Außenwirkung. Den bei Weitem größten Anteil haben dabei die präventiven Maßnahmen. Im Jahr 2009 wurden in ELBOS insgesamt 379.913 Maßnahmen registriert, davon 180.835 (48 %) präventive, 74.730 Maßnahmen im Rahmen der Strafverfolgung, 20.668 Verkehrsdelikte, 76.048 Verkehrsunfälle, 14.395 Maßnahmen im Zusammenhang mit zivilen Rechtsansprüchen sowie 13.237 interne. Für die nachfolgenden Analysen wurden als Vergleichsgröße die präventiven Polizeieinsätze zugrundegelegt. Diese wurden für den Evaluationszeitraum monatsweise aufbereitet.

*Tabelle 3: Einsatzzahlen in Relation zu der Gesamtzahl der präventiven Maßnahmen*

| Jahr | Monat | Präventive Zugriffe auf Verkehrsdaten | Präventive Einsätze insgesamt* | % |
|---|---|---|---|---|
| 2009 | Januar | 12 | 12.584 | 0,095 |
| 2009 | Februar | 18 | 12.068 | 0,149 |
| 2009 | März | 6 | 14.119 | 0,042 |
| 2009 | April | 13 | 16.077 | 0,081 |
| 2009 | Mai | 15 | 16.651 | 0,09 |
| 2009 | Juni | 13 | 14.769 | 0,088 |
| 2009 | Juli | 13 | 17.965 | 0,072 |
| 2009 | August | 15 | 18.248 | 0,082 |
| 2009 | September | 24 | 15.476 | 0,155 |
| 2009 | Oktober | 10 | 14.962 | 0,067 |
| 2009 | November | 8 | 13.937 | 0,057 |
| 2009 | Dezember | 10 | 13.979 | 0,072 |
| 2010 | Januar | 8 | 13.247 | 0,060 |
| 2010 | Februar | 14 | 11.556 | 0,121 |
| 2010 | März | 19 | 12.747 | 0,149 |
| 2010 | April | 17 | 13.114 | 0,129 |
| 2010 | Mai | 22 | 14.260 | 0,154 |
| 2010 | Juni | 21 | 13.631 | 0,154 |
| **insgesamt** | | **258** | **259.390** | **0,099** |

*) Gesamtzahl der Einsätze zur Gefahrenabwehr ohne Verkehrs- und sonstige Einsätze; Basis: ELBOS-Einsatznummern.

Entscheidender Parameter für die Beurteilung der Entwicklung im Bereich der präventiven Verkehrsdatenabfrage einschließlich der Mobilfunkortung ist nun der jeweilige Anteil dieser Maßnahmen an der Gesamtzahl der präventiven Einsätze. Die entsprechenden Werte ergeben sich im Einzelnen aus Tabelle 3. Es wird deutlich, dass sich die Zahl der Einsätze knapp im

Promillebereich bewegt. Im Durchschnitt machen diese Fälle gerade 0,099 % aller präventiven Einsätze aus. Die einzelnen Anteile schwanken zwischen 0,042 % und 0,154 %.

*Schaubild 2a: Entwicklung der Einsatzzahlen und der präventiven Maßnahmen insgesamt*

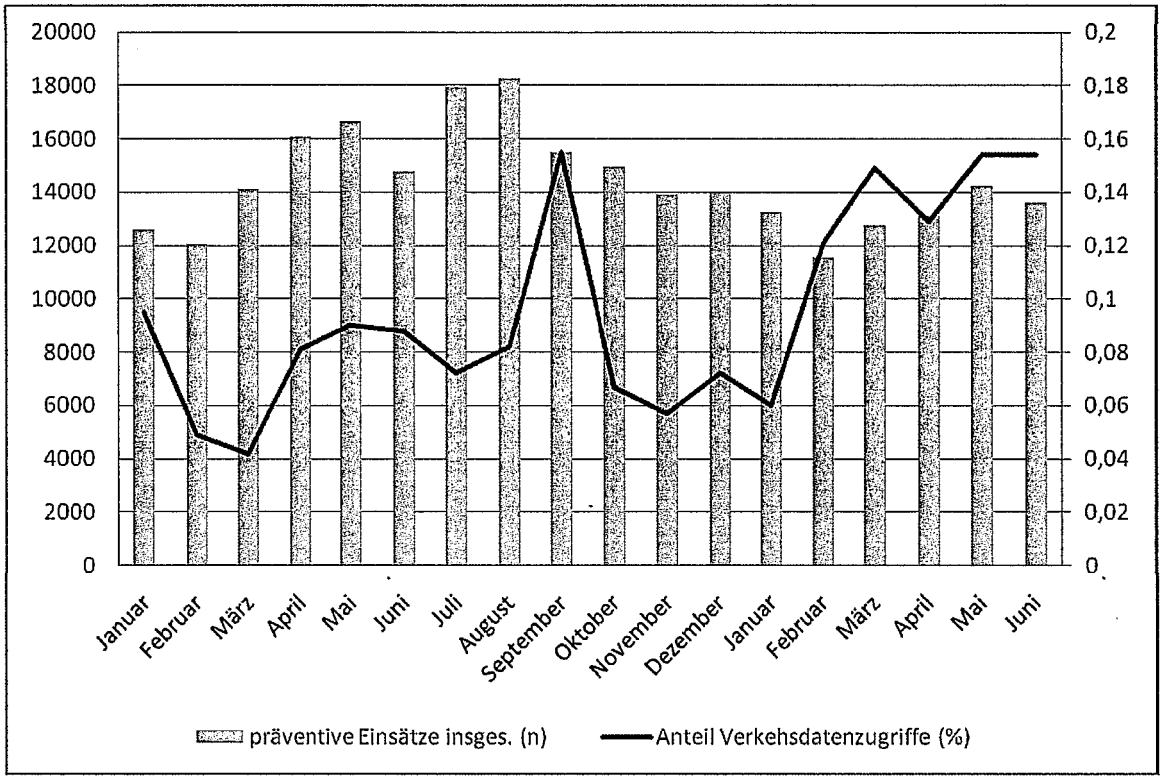
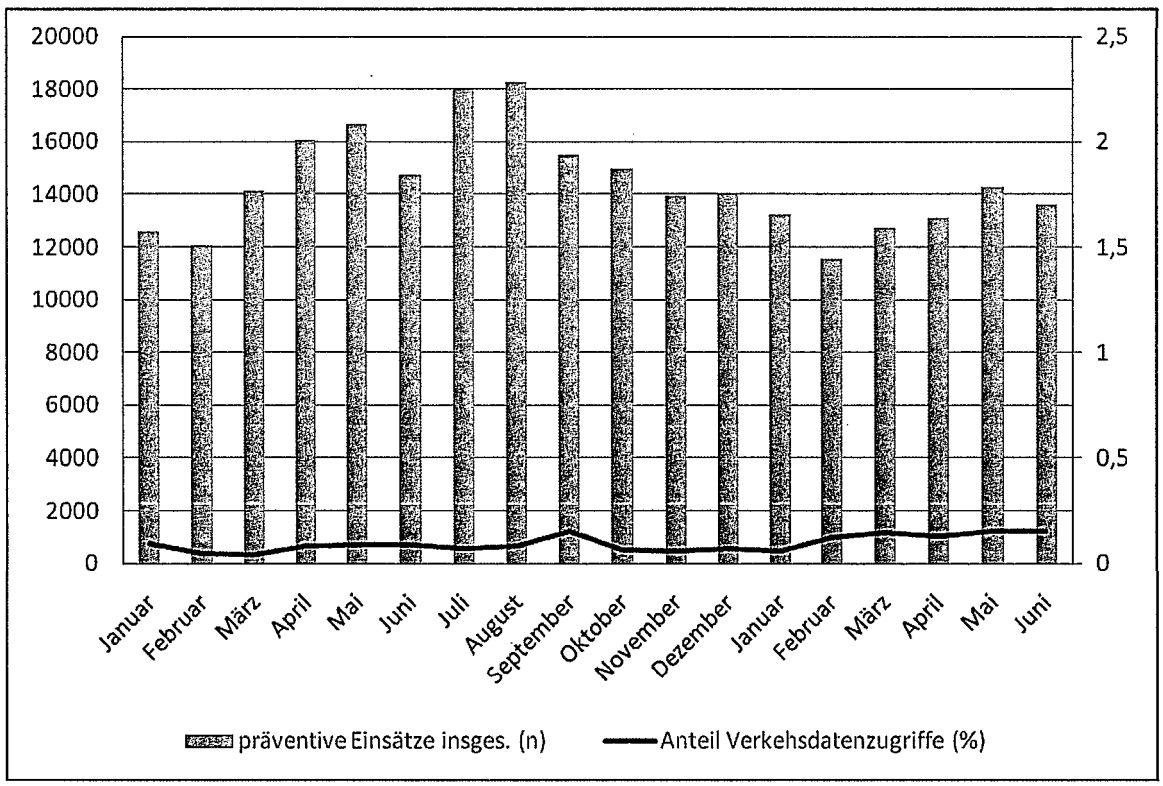



*Schaubild 2b: Entwicklung der Einsatzzahlen und der präventiven Maßnahmen insgesamt (2)*

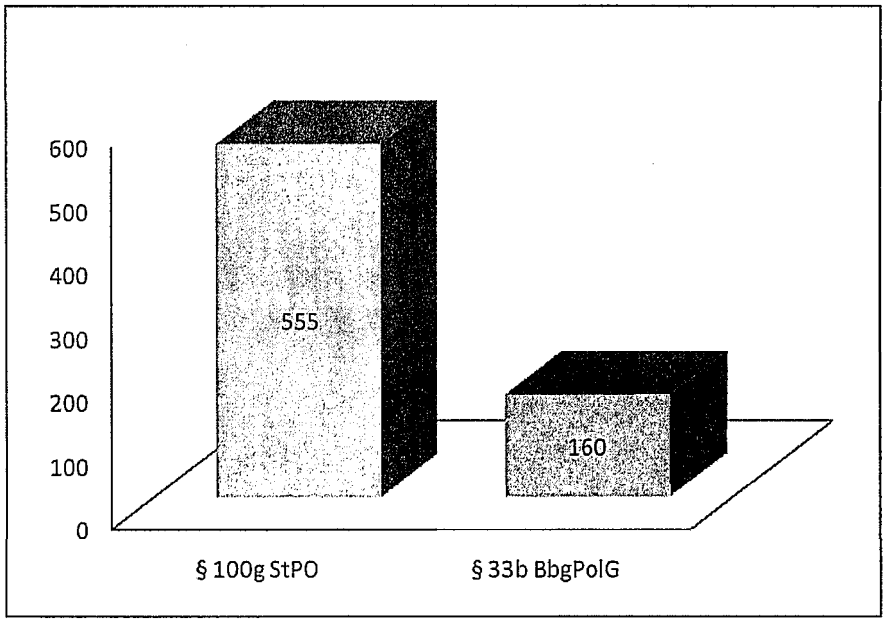


Diese relative Betrachtungsweise verändert das Gesamtbild und insbesondere die größeren Ausschläge, wie sie bereits auf der Grundlage der absoluten Zahlen aus Schaubild 1 herauszulesen waren, nicht grundlegend (Schaubild 2a). So wird die Zunahme, die sich bereits auf der Grundlage der absoluten Zahlen für die letzen beiden Quartale angedeutet hatte, auch hier sichtbar. Zum Ende des Evaluationszeitraumes haben sich die Werte erkennbar auf etwas höherem Niveau eingependelt. Der Vergleich der durchgezogenen Linie (prozentualer Anteil der Verkehrsdatenabfragen) mit den absoluten Zahlen zur Gesamtzahl der Einsätze (Säulen) zeigt aber auch, dass die Verläufe zwar in einigen Abschnitten ähnlich, aber nicht durchweg deckungsgleich sind. Dass die Schwankungen bei den Maßnahmen gem. § 33b Abs. 3 Nr. 2 und Abs. 6 S. 2 BbgPolG in Anbetracht der sehr niedrigen Fallzahlen ausgeprägter ausfallen als bei der Gesamtzahl der Einsätze, ist zwangsläufig und sollte nicht zur Überinterpretation verleiten.

Die Varianz wird im Übrigen weitgehend marginalisiert, wenn der Maßstab der Darstellung verändert wird. Ein solch veränderter Maßstab liegt Schaubild 2b zugrunde[294]. Als Intervall wurde hier der Bereich zwischen 0 und 2,5 % gewählt. Es ist derjenige, der bei der Analyse der Daten zur automatischen Kennzeichenfahndung zur Anwendung kam. Damit wird die Entwicklung beider Maßnahmen unmittelbar vergleichbar. Anders als im Fall der Kennzeichenfahndung (vgl. unten Schaubild 8) ergibt sich für die auf die Verkehrsdaten bezogenen Maßnahmen über den Evaluationszeitraum hinweg insgesamt ein nahezu gleichbleibend niedriges Niveau.

### *2.2 Verhältnis der präventiven zur repressiven Verkehrsdatenabfrage*

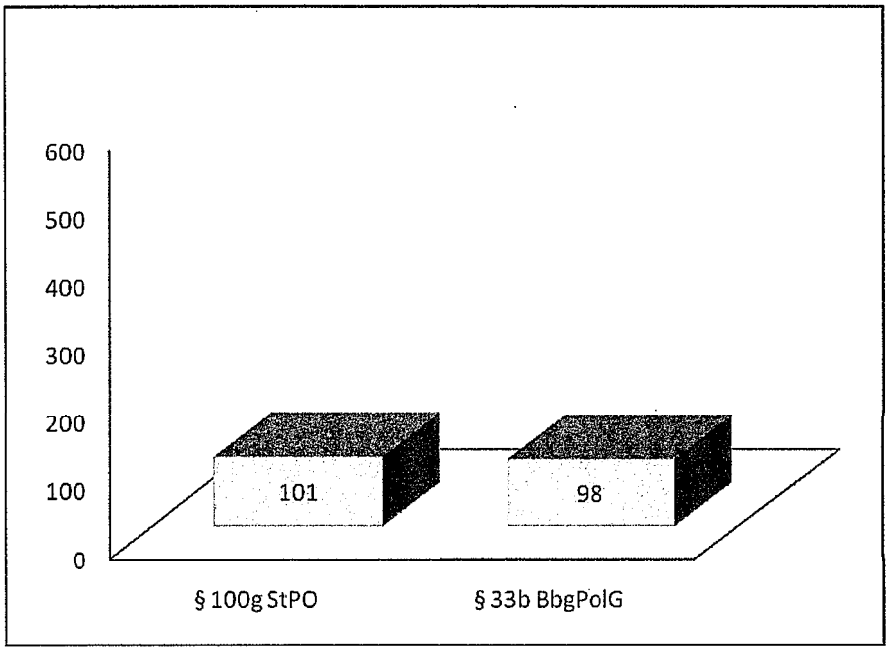
*Schaubild 3a: Repressive und präventive VDA in Brandenburg (2009)**




*) Angabe zu den repressiven Verkehrsdatenabfragen (VDA) nach Bundesamt für Justiz: Maßnahmen nach § 100g StPO für 2009, Ziff. 4 (Anzahl der Anordnungen in Brandenburg).

294 Siehe jeweils die rechte Vertikalachse.

*Schaubild 3b: Repressive und präventive VDA in Brandenburg (Januar bis Juni 2010)**




*) Angabe zu den repressiven Verkehrsdatenabfragen (VDA) nachrichtlich durch die Generalstaatsanwaltschaft Potsdam; die Gesamtstatistik des Bundesamtes für Justiz für das Jahr 2010 ist noch nicht verfügbar.

Die Anwendungszahlen bei den Maßnahmen gem. § 33b Abs. 3 Nr. 2 und Abs. 6 S. 2 BbgPolG liegen am Anfang auch deutlich niedriger als die repressive Einsatzvariante der Verkehrsdatenabfrage. Dies ergibt sich aus einem Vergleich mit der vom Bundesamt für Justiz jährlich veröffentlichten Statistik gem. § 100g Abs. 4 StPO[295]. Diese weist für Brandenburg für das Jahr 2009 insgesamt 555 Anordnungen gem. § 100g StPO aus. Somit machten die präventiven Anwendungen zu dieser Zeit etwa ein Fünftel aller Verkehrsdatenabfragen aus (22,4 %), die repressiven vier Fünftel (Schaubild 3a). Dies stellt sich im ersten Halbjahr 2010 signifikant anders dar. Nach den vorläufigen Zahlen für das Land Brandenburg wurden Verkehrsdaten nun etwa gleich häufig mit repressiver oder mit präventiver Zielrichtung abgefragt (Schaubild 3b). Dies spiegelt zum einen die leichte Zunahme der absoluten Anwendungsfälle bei den Maßnahmen gem. § 33b BbgPolG wider. Zum anderen ist aber gerade die Zahl der Maßnahmen nach § 100g StPO um mehr als die Hälfte zurückgegangen[296], was als unmittelbare Folgewirkung des Urteils des BVerfG vom 2.3.2010 zur Vorratsdatenspeicherung[297] und der damit einhergehenden Veränderungen in der Praxis[298] interpretiert werden kann.

---

[295] Vgl. www.bundesjustizamt.de/cln_108/nn_1635504/DE/Themen/Justizstatistik/Telekommunikationsueberwachung/downloads/Uebersicht__Verkehrsdaten__2009,templateId=raw,property=publicationFile.pdf/Uebersicht_Verkehrsdaten_2009.pdf

[296] Zur Verdeutlichung dieser Entwicklung wurde die Skalierung von Schaubild 3a übernommen. Zu beachten ist, dass Schaubild 3a die Jahreswerte abbildet, Schaubild 3b nur die Halbjahreswerte.

[297] BVerfG, 1 BvR 256/08 v. 2.3.2010, z.B. NJW 2010, S. 803, NStZ 2010, S. 341, NVwZ 2010, S. 770.

### *2.3 Anlass der Maßnahmen*

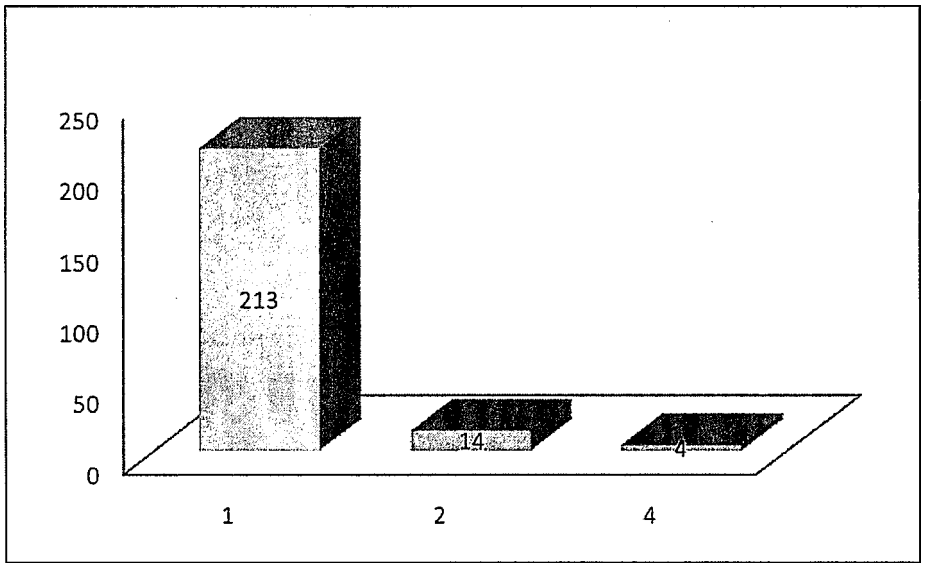
*Tabelle 4: Anzahl gefährdeter Personen**

| Anzahl Personen | Häufigkeit | % |
|---|---|---|
| 1 | 213 | 92,21 |
| 2 | 14 | 6,06 |
| 4 | 4 | 1,73 |
| **insgesamt** | **231** | **100** |

*) Missing values: 27 (10,5 %).

Anlass für die Durchführung der Maßnahmen war in allen 258 analysierten Fällen eine Gefahr für Leib oder Leben eines Menschen. Zumeist war eine einzelne Person in Gefahr, in 14 Fällen zwei und in vier Fällen vier Personen (Tabelle 4). Die prozentuale Verteilung ist aus Schaubild 4 ersichtlich. Ausweislich der beigezogenen Akten ergibt sich, dass in 10 Fällen Minderjährige in Gefahr waren, darunter waren vier Kinder jünger als 10 Jahre und zwei Babys im Alter von unter einem Jahr. Angekündigte Suizide oder vermutete Suizidabsichten, Unfallsituationen sowie akute Gewaltsituationen und vermutete oder tatsächliche Bedrohungssituationen für Leib oder Leben, ausgelöst durch strafrechtlich relevantes Verhalten Dritter, waren typische Anlasskonstellationen für die Maßnahmen. Einige exemplarische Sachverhalte sind in der nachfolgenden Übersicht 5 zusammengestellt.

*Schaubild 4: Anzahl gefährdeter Personen (2)*




298 Siehe dazu auch gleich unten Pkt. 2.5.

*Übersicht 5: Einige exemplarische Sachverhalte bei der Verkehrsdatenabfrage*

Die Betroffene wurde von ihren Eltern aus einer Psychiatrie abgeholt und sollte von ihnen in eine andere Psychiatrie gebracht werden. Sie litt unter Psychosen und sollte ab jetzt medikamentös behandelt werden. Als die Betroffene mit ihren Eltern gegen 23 Uhr den Eingang der neuen Psychiatrie erreichte, floh sie. Sofort eingeleitete Fahndungsmaßnahmen mittels Funkstreifenwagen und der Einsatz eines Fährtenhundes waren erfolglos. An ihrer Wohnanschrift wurde sie nicht angetroffen. Die Außentemperatur betrug ca. 0°C. Da die Betroffene keine Jacke bei sich führte, bestand unter anderem die Gefahr einer Unterkühlung.

Aufgrund schwerwiegender Beziehungsprobleme war es zwischen dem Betroffenen, der Polizeibeamter ist, und seiner Frau in der Vergangenheit immer wieder zu verbalen und körperlichen Auseinandersetzungen gekommen. Nach einer erneuten Auseinandersetzung im Urlaub drohte der Betroffene seiner Frau, er werde jetzt nach Hause fahren, seine Dienstwaffe holen und dann zuerst sie und anschließend sich selbst erschießen. Er fuhr mit seinem Pkw in unbekannte Richtung davon. Telefonisch war der Betroffene nicht zu erreichen, von suizidalen Absichten war auszugehen.

Nachdem der Betroffene mehrfach mit massiver Gewalt auf seine Lebensgefährtin eingewirkt hatte, hatte sich diese von ihm getrennt. Daraufhin drohte er seiner bisherigen Lebensgefährtin, dass er sie und ihre Angehörigen umbringen werde. Der Betroffene führte regelmäßig ein langes Messer bei sich und war im Besitz eines pistolenähnlichen Gegenstandes. Ob es sich hierbei um eine echte oder um eine Schreckschusswaffe handelte, war nicht bekannt.

Absturz eines einmotorigen Flugzeuges. Der Pilot war verletzt. Über sein Mobiltelefon sendete er einen Notruf aus. Mit Hilfe der abgefragten Standortdaten konnte die Absturzstelle lokalisiert werden.

Eine weibliche Person meldete über den polizeilichen Notruf, dass sie gegenwärtig von einem Mann verfolgt werde. Dieser habe sie bedroht und vergewaltigt bzw. wolle sie noch weiter vergewaltigen. Sie war offenbar in Todesangst und wusste nicht, wo sie sich befand. Während des Notrufes war im Hintergrund eine männliche Stimme „Steig ein!“ zu vernehmen. Dann brach das Telefonat ab.

Der Betroffene hat über sein Mobiltelefon angekündigt, sich das Leben nehmen zu wollen. Bei der durchgeführten Überprüfung seiner Adresse wurde ein Abschiedsbrief gefunden, aus dem eindeutige Suizidabsichten hervorgingen.

Der Betroffene verließ nach einem Verkehrsunfall zu Fuß den Unfallort und war anschließend nicht mehr auffindbar. Auf Grund der Unfallsituation konnte nicht ausgeschlossen werden, dass er sich bei dem Unfall Verletzungen zugezogen oder einen Schock davongetragen hat. An seiner Wohnanschrift wurde er nicht angetroffen. Alle Versuche der Kontaktaufnahme verliefen erfolglos. Aufgrund der Außentemperatur von ca. -10°C war von einer permanent steigenden Gefährdung der Person auszugehen.

Eine Frau rief von einem Mobiltelefon bei der Rettungsleitstelle an. Sie war nicht in der Lage, sich klar zu artikulieren. Auf Nachfragen antwortete sie nicht. Es waren deutlich Würgegeräusche, schmerzhaftes Stöhnen und Weinen zu hören. Der Notruf brach nach kurzer Zeit unvermittelt ab. Mehrere Rückrufe durch die Leitstelle verliefen erfolglos. Alle durchgeführten Fahndungsmaßnahmen einschließlich der Überprüfung der Wohnadresse der Telefonanschlussinhaberin verliefen ohne Erfolg. Die Wohnung war leer. Weitere Fahndungsansätze waren nicht ersichtlich oder wurden in Anbetracht der Dringlichkeit als nicht gleich erfolgversprechend eingestuft.

Die Ehefrau des Betroffenen erschien bei der Polizei und gab an, dass der von ihr in Trennung lebende Ehemann amerikanischer Staatsbürgerschaft mit ihren gemeinsamen Kindern unbekannten Aufenthaltes sei. Die Kinder hätten nach dem gemeinsamen Wochenende mit dem Vater absprachegemäß zur Mutter zurückgebracht werden sollen, was nicht geschah. Der Ehemann hatte kurz zuvor geäußert, dass die Kinder besser tot wären als in Deutschland zu bleiben. Der Ehemann war im Besitz einer Schusswaffe. In der Wohnung des Betroffenen wurde niemand angetroffen.

Der Betroffene holte seinen dreieinhalbjährigen Sohn von der Mutter (ehemalige Lebensgefährtin des Betroffenen) ab, um mit diesem spazieren zu gehen. In der Vergangenheit hatte der Vater das Kind stets pünktlich zurückgebracht. Zwischen dem Gesuchten und der Kindesmutter gab es keinen Streit. Abends informierte die derzeitige Freundin des Betroffenen dessen ehemalige Lebensgefährtin telefonisch darüber, dass sie mit dem Betroffenen telefonischen Kontakt gehabt hatte. Dieser habe ihr erzählt, dass er mit seinem Kind auf dem Eis spazieren sei. Plötzlich habe es ein lautes Geräusch gegeben, nach dem das Gespräch plötzlich abbrach. Alle weiteren Versuche, telefonischen Kontakt mit dem Betroffenen herzustellen, schlugen fehl. Es bestand die dringende Gefahr, dass dieser mit dem Kind in das Eis eingebrochen ist.

Ein Zweifamilienhaus war eingestürzt. Zu der Zeit des Unglücks war ein Bewohner des Hauses mit einem Freund verabredet gewesen. Telefonisch konnte der Betroffene nicht erreicht werden. Mithilfe der Funkzellenabfrage sollte ausgeschlossen werden, dass sich der Betroffene unter den Trümmern befindet.

Der Betroffene meldete sich über den Notruf bei der Rettungsleitstelle und teilte dieser mit, dass er unter einem Baum liege und sich aus eigener Kraft nicht befreien könne. Seinen Aufenthaltsort konnte er der Rettungsleitstelle nicht mitteilen. Versuche, die Person zurückzurufen, blieben ohne Erfolg. Auf Grund dieser Tatsachen musste davon ausgegangen werden, dass sich der Gesuchte in einem hilflosen, möglicherweise lebensbedrohlichen Zustand befindet.

Die psychologische und die gesetzlich bestellte Betreuerin teilen der Polizei zeitgleich mit, dass sich die Betroffene das Leben nehmen wolle. Sie leide an einer psychischen Erkrankung und es bestehe Suizidgefahr. In einem Telefonat gab die Betroffene an, sich mit Tabletten das Leben nehmen zu wollen. Auf Nachfrage der Psychologin, ob sie die kommende Nacht überstehe, ohne sich etwas anzutun, antwortete die Betroffene, sie glaube das nicht.

Die Betroffene meldete sich telefonisch bei ihrem Ehemann und gab glaubhaft an, sich in einem Waldstück zu befinden, um sich etwas anzutun. Nach diesem Gespräch gelang es dem Anschlussinhaber nicht mehr, seine Frau telefonisch zu erreichen. Das Telefon klingelte zwar, sie nahm aber nicht ab. Die Betroffene hatte etwa ein halbes Jahr vorher bereits versucht, sich in ihrer Wohnung mit Tabletten das Leben zu nehmen. Seither befand sie sich in psychologischer Betreuung und nahm Antidepressiva ein.

Die betroffene Jugendliche wurde seit drei Tagen vermisst. Sie hatte ihrem Vater eine E-Mail mit folgendem Inhalt geschrieben: „Papa, holt mich schnell raus! Der lässt mich nicht mehr weg und ich muss ständig Zeug rauchen. Und mit seinen Freunden muss ich auch schlafen oder er schlägt mich."

### *2.4 Durchführung der Maßnahmen*

Mehrheitlich wurden die Maßnahmen, dem gesetzlichen Grundsatz entsprechend, vorab bei dem zuständigen Amtsgericht beantragt. In knapp 44 % der Fälle wurde dagegen Gefahr im Verzug im Sinne von § 33b Abs. 5 S. 1 BbgPolG angenommen und die Maßnahme durch das Polizeipräsidium angeordnet. Die genaue Anzahl für die beiden Konstellationen ergibt sich aus Tabelle 5. Zumindest in den 223 Fällen, für die aussagekräftige Informationen hierzu vorhanden waren, wurde die richterliche Bestätigung in den Eilfällen nachträglich eingeholt. Über die Praxis in den Fällen, zu denen keine entsprechenden Informationen vorlagen (n = 35), kann zu diesem Punkt keine Angabe gemacht werden.

*Tabelle 5: Anordnende Behörde**

| Anordnende Behörde | Anzahl | % |
|---|---|---|
| Gericht | 124 | 55,61 |
| Polizeipräsidium | 99 | 44,39 |
| **insgesamt** | **223** | **100** |

*) Missing values: 35 (13,6 %).

*Tabelle 6: Anzahl betroffener Mobilanschlüsse**

| Anzahl | Anzahl | % |
|---|---|---|
| Ein Anschluss | 193 | 99,5 |
| Zwei Anschlüsse | 1 | 0,5 |
| **insgesamt** | **194** | **100** |

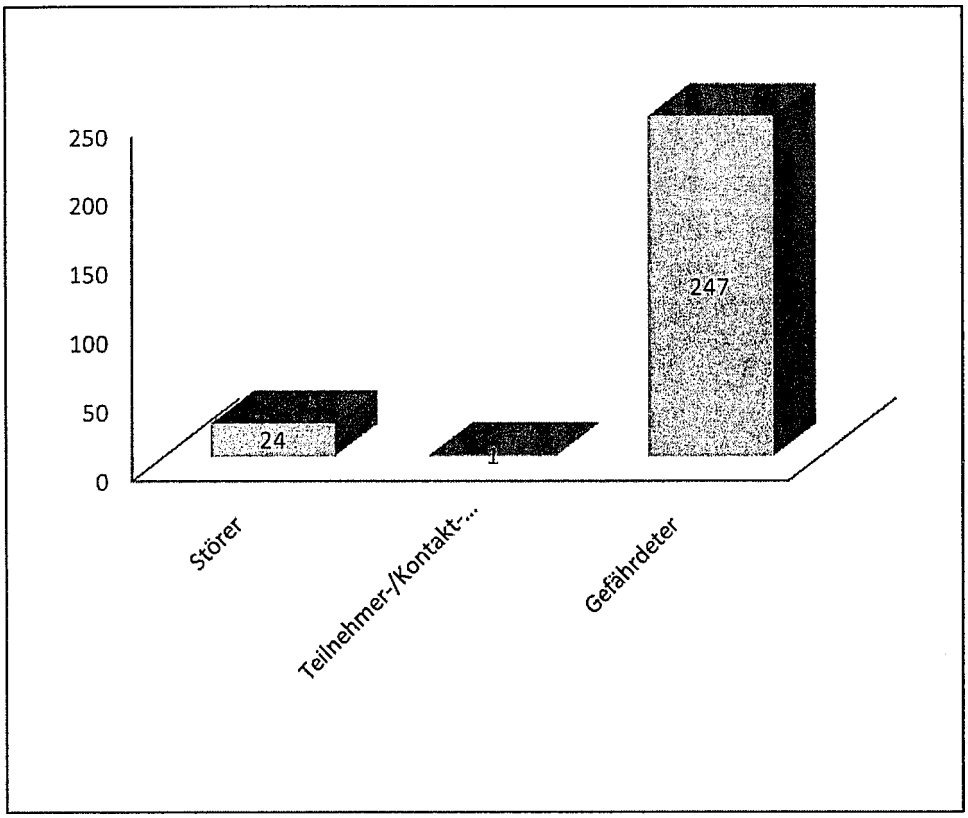
*) Missing values: 64 (24,8 %).

Die Abfrage erfolgte in den meisten Fällen auch sehr zielgenau, indem jeweils nur die Standortdaten eines konkreten Mobilanschlusses abgefragt wurden (Tabelle 6). Nur in einem Fall war die Abfrage auf zwei verschiedene Handys, die eine gefährdete Person möglicherweise bei sich hätte tragen können, gerichtet. In 64 Fällen waren den Unterlagen keine verlässlichen Angaben zu dieser Frage zu entnehmen.

Auch die Analyse der Zielpersonen, die bzw. deren Mobiltelefone von der Abfrage betroffen waren, entspricht sehr gut der Zusammensetzung der zugrundeliegenden Fallkonstellationen. Im Mittelpunkt stehen ganz eindeutig die gefährdeten Personen, sei es in hilflosen Situationen oder Situationen der Selbstgefährdung, die die Mehrzahl der Fälle ausmachen, sei es in Bedrohungssituationen, wo der Gefährder bzw. Störer oftmals (noch) nicht identifiziert ist. Hier bleibt dann als einziges zielführendes bzw. erfolgversprechendes Mittel der Zugriff auf das Mobiltelefon des Opfers. Entsprechend gestaltet sich die Verteilung der Zielpersonen in den analysierten Fällen (Schaubild 5). Danach erfolgte die Standortdatenabfrage in 90 %

der Fälle für das Handy der gefährdeten Person. Diese Praxis ist durch die aktuelle Fassung des § 33b Abs. 2 S. 1 BbgPolG seit der Neufassung durch das Vierte Gesetz zur Änderung des Brandenburgischen Polizeigesetzes ausdrücklich gedeckt[299].

*Schaubild 5: Zielpersonen der Verkehrsdatenabfrage (2)*




In den meisten übrigen Fällen wurde auf die Geodaten beim Störer zugegriffen. Teilnehmer sowie Kontakt- oder Begleitpersonen spielten fast keine Rolle. Die genaue Verteilung ergibt sich aus Tabelle 7; sie enthält Mehrfachnennungen. So war in sieben Fällen sowohl das Mobiltelefon der gefährdeten Person als auch das des mutmaßlichen Gefährders (Störers) Gegenstand der Maßnahme. Belastbare Informationen über mögliche Folgemaßnahmen für die Störer waren den Akten nicht zu entnehmen.

Insgesamt ergibt sich auf der Basis der zuletzt dargestellten Parameter – Anzahl der betroffenen Anschlüsse und Kreis der Zielpersonen – eine sehr begrenzte Eingriffsbreite der Maßnahmen. Unbeteiligte waren praktisch nicht betroffen. Und für den Kreis der Betroffenen selbst ergibt sich eine Eingriffstiefe, die sich auf das zur Abwehr der Gefahr absolut Notwendige beschränkt. In allen dokumentierten Fällen erfolgte lediglich eine Abfrage, gerichtet auf vorhandene (Standort-)Daten. Hingegen fand insbesondere die gesetzlich ebenfalls zulässige

---

[299] Viertes Gesetz zur Änderung des Brandenburgischen Polizeigesetzes vom 18.12.2006, Gesetz- und Verordnungsblatt, Teil I – Nr. 18 vom 20.12.2006, S. 188. Vgl. hierzu Landtags-Drucksache 4/3508, S. 34.

Variante der Erhebung erst künftig anfallender Verkehrsdaten, die der Maßnahme ein anderes Gepräge im Sinne einer längerfristigen Überwachung verleihen und damit auch die Eingriffstiefe intensivieren würde, keine Anwendung.

*Tabelle 7: Zielpersonen der Verkehrsdatenabfrage*

| Zielperson* | Anzahl | % |
|---|---|---|
| Störer | 24 | 8,82 |
| Teilnehmer-/Kontakt-/Begleitperson | 1 | 0,37 |
| Gefährdeter | 247 | 90,81 |
| **insgesamt** | **272** | **100** |

*) Mehrfachnennungen.

### *2.5 Ergebnis der Verkehrsdatenabfragen*

In der großen Mehrzahl der Fälle konnten die abgefragten Standortdaten bei den Telekommunikationsanbietern auch ermittelt werden, und zwar in 91 % der Fälle vollständig sowie in zwei weiteren Fällen (ca. 1 %) zumindest teilweise (Tabelle 8). In 16 Fällen war das Auskunftsbegehren der Polizei erfolglos. Dabei erfolgte in mehreren Fällen tatsächlich keine oder keine rechtzeitige Rückmeldung, einmal war bei dem Netzbetreiber trotz mehrmaliger telefonischer Nachfrage niemand erreichbar; von dort kam auch kein Rückruf. Häufiger waren allerdings negative Rückmeldungen. Dies betrifft Fälle, in denen das gesuchte Mobiltelefon dauernd oder jedenfalls in Zeitnähe zu dem relevanten Abfragezeitpunkt ausgeschaltet war und die abgefragten Standortdaten daher nicht generiert werden konnten. In Schaubild 6 ist das Auskunftsverhalten auch grafisch aufbereitet.

*Tabelle 8: Beauskunftung durch die Telekommunikationsunternehmen*

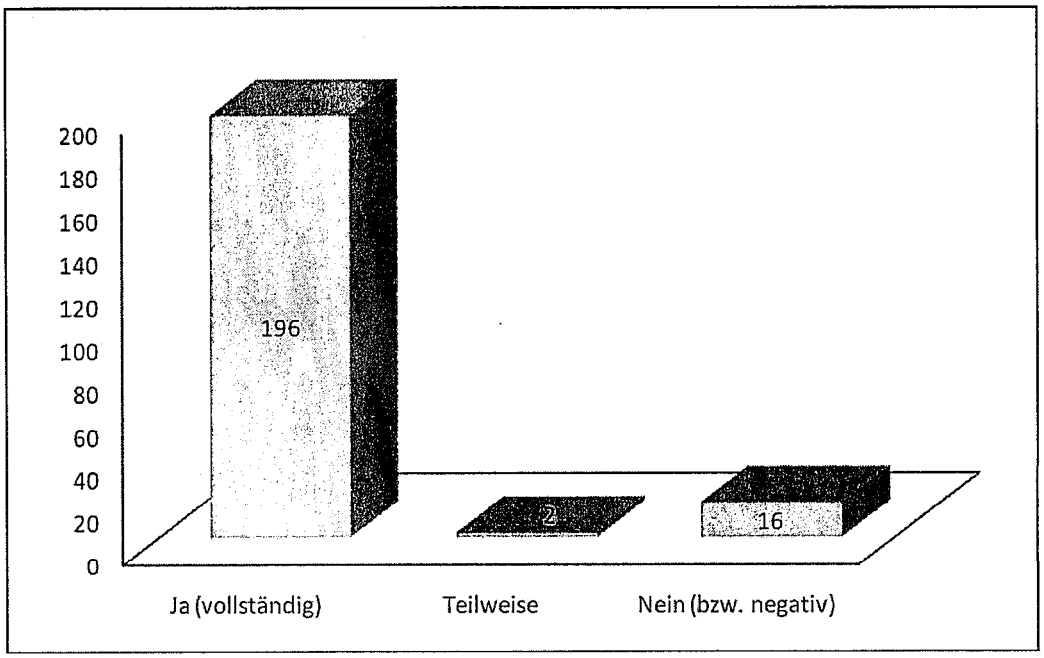
| Beauskunftung | Anzahl | % |
|---|---|---|
| Ja (vollständig) | 196 | 91,59 |
| Teilweise | 2 | 0,93 |
| Nein (bzw. negativ) | 16 | 7,48 |
| **Insgesamt** | **214** | **100** |

*) Missing values: 44 (17,1 %).

Zu beachten ist allerdings, dass diese Befunde größtenteils die Situation vor dem Urteil des BVerfG vom März 2010 zur Vorratsdatenspeicherung widerspiegeln. In Reaktion auf das Urteil haben sich sowohl das Auskunftsverhalten als auch die Speicherpraxis der Unternehmen verändert. Die inzwischen deutlich verkürzten Speicherfristen dürften sich auf die Fälle der unmittelbaren Gefahrenabwehr freilich nicht in nennenswertem Umfang auswirken. Denn für eine kurze Zeitspanne von etwa sieben Tagen sind die Daten bei den allermeisten Anbietern auch heute noch verfügbar, sodass die Standortdatenabfrage, die im Gefahrenfall ja in aller Regel auf Echtzeitdaten bezogen ist, als Maßnahme der Gefahrenabwehr jedenfalls grundsätzlich auch weiterhin verfügbar sein dürfte. Allerdings ist auch das Auskunftsverhalten der Anbieter restriktiver geworden. Im Rahmen von Interviews, die für ein anderes For-

schungsprojekt des Max-Planck-Instituts[300] mit Polizeipraktikern aus allen Bundesländern durchgeführt wurden, wurde berichtet, dass sich Unternehmen zumindest in Einzelfällen auch in akuten Gefahrensituationen weigerten, Verkehrsdatenabfragen zu beauskunften, wenn sie die gesetzlichen Voraussetzungen für die Eilanordnungsbefugnis als nicht gegeben betrachteten. Problematisch erscheinen dabei insbesondere solche Fälle, in denen ein Telekommunikationsunternehmen mit Sitz in einem anderen Bundesland das am Einsatzort gültige Landespolizeigesetz nicht als maßgebliche Rechtsgrundlage anerkennt.

*Schaubild 6: Beauskunftung durch die Telekommunikationsunternehmen (2)*




### *2.6 Gesamtbilanz: Überwachungssituation in Brandenburg während des Evaluationszeitraumes im Hinblick auf die präventive Verkehrsdatenabfrage*

Abschließend wurden zur Erstellung einer Art Gesamtbilanz der Überwachungssituation im Hinblick auf die präventive Verkehrsdatenabfrage sämtliche Maßnahmen gem. § 33b Abs. 3 Nr. 2 und Abs. 6 S. 2 BbgPolG für den Evaluationszeitraum tagesgenau zusammengestellt. Das Ergebnis ist in Tabelle 9 in Kalenderform dargestellt. Dies greift einen Ansatz *Roßnagels*[301] auf, der aus der Rechtsprechung des BVerfG zu den verdeckten Überwachungsmaßnahmen die Pflicht zu einer kumulativen Bewertung der Überwachungslast für den Bürger ableitet.

---

[300] Im Sommer 2011 wird das Gutachten des Max-Planck-Instituts für ausländisches und internationales Strafrecht „Schutzlücken durch Wegfall der Vorratsdatenspeicherung?" vorliegen. Die Untersuchung ist derzeit noch in Bearbeitung.

[301] *Roßnagel*, NJW 2010, S. 1238. Die hier vorgelegte Übersicht wäre allerdings nur ein einzelner „Rechnungsposten" einer entsprechenden Überwachungs-Gesamtrechnung. Eine solche soll und kann hier mit Blick auf den begrenzten Untersuchungsauftrag freilich nicht erstellt werden.

*Tabelle 9: Anzahl der präventiven Verkehrsdatenzugriffe in Brandenburg für jeden Tag des Evaluationszeitraumes*

| 2009 | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Januar** | **Montag** | **Dienstag** | **Mittwoch** | **Donnerstag** | **Freitag** | **Samstag** | **Sonntag** |
| **KW 1** | | | | 1 | 0 | 1 | 0 |
| **KW 2** | 1 | 1 | 0 | 0 | 1 | 0 | 0 |
| **KW 3** | 0 | 0 | 1 | 0 | 0 | 1 | 0 |
| **KW 4** | 0 | 0 | 0 | 0 | 1 | 1 | 0 |
| **KW 5** | 0 | 0 | 0 | 2 | 1 | 0 | |

| **Febuar** | **Montag** | **Dienstag** | **Mittwoch** | **Donnerstag** | **Freitag** | **Samstag** | **Sonntag** |
|---|---|---|---|---|---|---|---|
| **KW 5** | | | | | | | 0 |
| **KW 6** | 0 | 0 | 0 | 3 | 2 | 0 | 0 |
| **KW 7** | 0 | 1 | 2 | 0 | 0 | 1 | 1 |
| **KW 8** | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| **KW 9** | 2 | 1 | 1 | 0 | 1 | 0 | |

| **März** | **Montag** | **Dienstag** | **Mittwoch** | **Donnerstag** | **Freitag** | **Samstag** | **Sonntag** |
|---|---|---|---|---|---|---|---|
| **KW 9** | | | | | | | 0 |
| **KW 10** | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| **KW 11** | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| **KW 12** | 2 | 0 | 0 | 0 | 1 | 0 | 0 |
| **KW 13** | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| **KW 14** | 0 | 0 | | | | | |

| **April** | **Montag** | **Dienstag** | **Mittwoch** | **Donnerstag** | **Freitag** | **Samstag** | **Sonntag** |
|---|---|---|---|---|---|---|---|
| **KW 14** | | | 0 | 1 | 0 | 0 | 0 |
| **KW 15** | 1 | 0 | 1 | 0 | 0 | 2 | 1 |
| **KW 16** | 0 | 0 | 0 | 0 | 0 | 0 | 2 |
| **KW 17** | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| **KW 18** | 1 | 1 | 2 | 0 | | | |

| **Mai** | **Montag** | **Dienstag** | **Mittwoch** | **Donnerstag** | **Freitag** | **Samstag** | **Sonntag** |
|---|---|---|---|---|---|---|---|
| **KW 18** | | | | | 0 | 0 | 0 |
| **KW 19** | 2 | 0 | 1 | 0 | 1 | 0 | 0 |
| **KW 20** | 0 | 0 | 1 | 1 | 0 | 0 | 0 |
| **KW 21** | 0 | 1 | 1 | 0 | 2 | 0 | 1 |
| **KW 22** | 1 | 1 | 1 | 0 | 1 | 0 | 0 |

| **Juni** | **Montag** | **Dienstag** | **Mittwoch** | **Donnerstag** | **Freitag** | **Samstag** | **Sonntag** |
|---|---|---|---|---|---|---|---|
| **KW 23** | 0 | 1 | 0 | 2 | 2 | 0 | 0 |
| **KW 24** | 0 | 1 | 0 | 0 | 0 | 0 | 1 |
| **KW 25** | 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| **KW 26** | 0 | 2 | 0 | 0 | 0 | 1 | 1 |
| **KW 27** | 1 | 0 | | | | | |

| Juli | Montag | Dienstag | Mittwoch | Donnerstag | Freitag | Samstag | Sonntag |
|---|---|---|---|---|---|---|---|
| KW 27 | | | 1 | 0 | 0 | 0 | 0 |
| KW 28 | 1 | 1 | 0 | 1 | 0 | 4 | 0 |
| KW 29 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| KW 30 | 0 | 1 | 1 | 2 | 1 | 0 | 0 |
| KW 31 | 0 | 0 | 0 | 0 | 0 | | |

| August | Montag | Dienstag | Mittwoch | Donnerstag | Freitag | Samstag | Sonntag |
|---|---|---|---|---|---|---|---|
| KW 31 | | | | | | 0 | 1 |
| KW 32 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| KW 33 | 0 | 0 | 0 | 1 | 0 | 0 | 2 |
| KW 34 | 1 | 1 | 0 | 0 | 0 | 1 | 0 |
| KW 35 | 2 | 1 | 0 | 1 | 0 | 0 | 0 |
| KW 36 | 4 | | | | | | |

| September | Montag | Dienstag | Mittwoch | Donnerstag | Freitag | Samstag | Sonntag |
|---|---|---|---|---|---|---|---|
| KW 36 | | 3 | 1 | 2 | 0 | 0 | 0 |
| KW 37 | 0 | 2 | 2 | 1 | 0 | 0 | 1 |
| KW 38 | 2 | 0 | 2 | 1 | 0 | 0 | 0 |
| KW 39 | 3 | 0 | 0 | 2 | 1 | 0 | 0 |
| KW 40 | 1 | 0 | 0 | | | | |

| Oktober | Montag | Dienstag | Mittwoch | Donnerstag | Freitag | Samstag | Sonntag |
|---|---|---|---|---|---|---|---|
| KW 40 | | | | 1 | 0 | 0 | 1 |
| KW 41 | 0 | 1 | 0 | 1 | 1 | 0 | 1 |
| KW 42 | 0 | 1 | 0 | 1 | 0 | 0 | 0 |
| KW 43 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| KW 44 | 0 | 0 | 0 | 0 | 1 | 0 | |

| November | Montag | Dienstag | Mittwoch | Donnerstag | Freitag | Samstag | Sonntag |
|---|---|---|---|---|---|---|---|
| KW 44 | | | | | | | 0 |
| KW 45 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| KW 46 | 1 | 0 | 1 | 0 | 0 | 0 | 2 |
| KW 47 | 1 | 1 | 0 | 0 | 1 | 0 | 0 |
| KW 48 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| KW 49 | 0 | | | | | | |

| Dezember | Montag | Dienstag | Mittwoch | Donnerstag | Freitag | Samstag | Sonntag |
|---|---|---|---|---|---|---|---|
| KW 49 | | 0 | 0 | 0 | 1 | 1 | 0 |
| KW 50 | 1 | 2 | 0 | 0 | 0 | 0 | 0 |
| KW 51 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| KW 52 | 0 | 0 | 0 | 1 | 1 | 1 | 0 |
| KW 53 | 0 | 0 | 0 | 0 | | | |

| 2010 |
|---|

| Januar | Montag | Dienstag | Mittwoch | Donnerstag | Freitag | Samstag | Sonntag |
|---|---|---|---|---|---|---|---|
| KW 53 | | | | | 0 | 0 | 1 |
| KW 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| KW 2 | 1 | 0 | 0 | 0 | 1 | 1 | 1 |
| KW 3 | 1 | 0 | 1 | 0 | 0 | 0 | 0 |
| KW 4 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |

| Febuar | Montag | Dienstag | Mittwoch | Donnerstag | Freitag | Samstag | Sonntag |
|---|---|---|---|---|---|---|---|
| KW 5 | 0 | 0 | 1 | 1 | 0 | 1 | 1 |
| KW 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| KW 7 | 0 | 2 | 1 | 0 | 0 | 0 | 3 |
| KW 8 | 0 | 0 | 1 | 0 | 1 | 0 | 2 |

| März | Montag | Dienstag | Mittwoch | Donnerstag | Freitag | Samstag | Sonntag |
|---|---|---|---|---|---|---|---|
| KW 9 | 1 | 0 | 0 | 1 | 0 | 1 | 0 |
| KW 10 | 0 | 0 | 0 | 1 | 0 | 0 | 1 |
| KW 11 | 1 | 0 | 1 | 0 | 1 | 0 | 3 |
| KW 12 | 2 | 0 | 2 | 1 | 1 | 0 | 1 |
| KW 13 | 0 | 0 | 1 | | | | |

| April | Montag | Dienstag | Mittwoch | Donnerstag | Freitag | Samstag | Sonntag |
|---|---|---|---|---|---|---|---|
| KW 13 | | | | 1 | 1 | 1 | 0 |
| KW 14 | 0 | 3 | 0 | 0 | 0 | 1 | 0 |
| KW 15 | 0 | 0 | 2 | 2 | 1 | 0 | 0 |
| KW 16 | 0 | 0 | 0 | 0 | 0 | 0 | 3 |
| KW 17 | 0 | 1 | 1 | 0 | 0 | | |

| Mai | Montag | Dienstag | Mittwoch | Donnerstag | Freitag | Samstag | Sonntag |
|---|---|---|---|---|---|---|---|
| KW 17 | | | | | | 0 | 2 |
| KW 18 | 0 | 0 | 2 | 0 | 1 | 1 | 0 |
| KW 19 | 2 | 0 | 0 | 1 | 1 | 2 | 0 |
| KW 20 | 0 | 2 | 0 | 0 | 2 | 0 | 1 |
| KW 21 | 0 | 0 | 2 | 0 | 0 | 1 | 1 |
| KW 22 | 1 | | | | | | |

| Juni | Montag | Dienstag | Mittwoch | Donnerstag | Freitag | Samstag | Sonntag |
|---|---|---|---|---|---|---|---|
| KW 22 | | 1 | 1 | 0 | 1 | 0 | 2 |
| KW 23 | 0 | 0 | 0 | 1 | 0 | 4 | 0 |
| KW 24 | 1 | 0 | 1 | 0 | 1 | 1 | 0 |
| KW 25 | 3 | 0 | 0 | 0 | 0 | 1 | 0 |
| KW 26 | 0 | 3 | 0 | | | | |

In der Zusammenschau ergibt sich, dass an 174 Tagen gar keine Maßnahme durchgeführt wurde, an 143 Tagen je eine, an 38 Tagen zwei und an 9 Tagen drei Maßnahmen; der Höchstwert von vier Maßnahmen an ein und demselben Tag wurde insgesamt dreimal registriert. Es gab auch Kalenderwochen, in denen keine einzige Maßnahme durchgeführt wurde. Insgesamt kann aus dieser Überwachungsdichte eine nennenswerte Belastungssituation nicht abgeleitet werden.

## 3. Anlassbezogene automatische Kennzeichenfahndung

### *3.1 Anzahl der Einsätze und Entwicklung der Einsatzzahlen*

Im Gegensatz zu der präventiven Verkehrsdatenabfrage ergeben sich für die anlassbezogene automatische Kennzeichenfahndung gem. § 36a BbgPolG (AKF) deutlich höhere Anwendungszahlen sowie auf der Zeitachse eine signifikant andere Entwicklung in der Anwendungshäufigkeit. Dies wird bereits aus den Basiszahlen in Tabelle 10 deutlich. Danach wurden im Jahr 2009 insgesamt 545 Einsätze durchgeführt, 2010 waren es 2.479. Von diesen fallen 1.484 in den Evaluationszeitraum, der mit dem 30.9.2010 endete. Diesem Anstieg der Maßnahmen um das etwa Vierfache steht ein geringfügiger Rückgang der maßgeblichen Gesamtzahl der polizeilichen Einsätze in Brandenburg gegenüber.

*Tabelle 10: Fallzahlen der Automatischen Kennzeichenfahndung und polizeiliche Einsätze insgesamt (2009 und 2010)*

| Jahr | Einsätze AKF | Polizeiliche Einsätze insgesamt* |
|---|---|---|
| 2009 | 545 | 255.262 |
| 2010 | 2.479** | 228.975 |

*) Gesamtzahl der Einsätze zur Gefahrenabwehr und Strafverfolgung ohne Verkehrs- und sonstige Einsätze; Basis: ELBOS-Einsatznummern.
**) Davon 995 im vierten Quartal 2010; diese Fälle fallen nicht mehr in die Evaluation.

Die Vergleichsbasis wurde auch hier wieder aus den ELBOS-Einsatzzahlen generiert[302]. Anders als bei der Analyse der Verkehrsdatenabfrage wurde hier jedoch die Gesamtzahl der präventiven und der repressiven Einsätze zugrundegelegt. Dieser abweichende Maßstab war im Hinblick auf die besondere Fallstruktur der automatischen Kennzeichenfahndung zu wählen. Denn wegen des überwiegenden Einsatzes in Fällen des Fahrzeugdiebstahls (sog. Totalentwendung), der nach gegenwärtiger Rechtslage in Brandenburg ausschließlich auf der Grundlage von § 100h Abs. 1 S. 1 Nr. 2 StPO erfolgt[303], müssen die repressiven Einsätze mit berücksichtigt werden. Eine beschränkte Evaluation der ausschließlich präventiv orientierten Maßnahmen gem. § 36a BbgPolG hätte kein realitätsnahes Abbild der Einsatzpraxis erbracht.

---

302 Vgl. oben Pkt. 2.1.

303 Siehe oben Teil D Pkt. 3.

*Tabelle 11: Automatische Kennzeichenfahndung – Anwendungshäufigkeit im Evaluationszeitraum (Jan. 2009 bis Sept. 2010)*

| Jahr | Monat | Einsätze AKF |
|---|---|---|
| 2009 | Januar | 17 |
| 2009 | Februar | 20 |
| 2009 | März | 44 |
| 2009 | April | 39 |
| 2009 | Mai | 33 |
| 2009 | Juni | 31 |
| 2009 | Juli | 34 |
| 2009 | August | 32 |
| 2009 | September | 35 |
| 2009 | Oktober | 61 |
| 2009 | November | 106 |
| 2009 | Dezember | 93 |
| 2010 | Januar | 89 |
| 2010 | Februar | 104 |
| 2010 | März | 142 |
| 2010 | April | 152 |
| 2010 | Mai | 155 |
| 2010 | Juni | 173 |
| 2010 | Juli | 179 |
| 2010 | August | 241 |
| 2010 | September | 249 |
| **insgesamt** | | **2.029** |

In Tabelle 11 werden alle Maßnahmen, die im Rahmen der Evaluation untersucht wurden, wiederum monatsgenau für die Dauer des Evaluationszeitraumes ausgewiesen (n = 2.029). Diese Aufstellung lässt bereits deutlich werden, dass die Anwendungshäufigkeit in dieser Zeit nahezu kontinuierlich von Monat zu Monat zugenommen hat. Der Mittelwert von 97 Fällen wurde zunächst im November 2009 einmalig und dann ab Februar 2010 endgültig überschritten. Lagen die Einsatzzahlen in den ersten 9 Monaten 2009 meist noch sehr deutlich unter 50, näherten sie sich gegen Ende des Untersuchungszeitraumes (August und September 2010) knapp der Marke von 250. Das ist ein Vielfaches des Ausgangswertes von 17 vom Januar 2009.

Dieser nominale Anstieg wird aus Schaubild 7 deutlich sichtbar. Anders als im Fall der Verkehrsdatenabfrage mit ihrem sehr disparaten zeitlichen Verlauf (vgl. oben Schaubild 1) zeigt sich hier über den Zeitverlauf hinweg eine nahezu kontinuierliche und im Ausmaß wachsende Zunahme der Anwendungszahlen. Besonders deutlich fällt der Anstieg zwischen September und November 2009, Februar und April 2010 sowie vom Juli zum August 2010 aus. Die ersten beiden Phasen fallen mit der parallelen Zunahme der verfügbaren Geräte zusammen (siehe unten Schaubild 13), die letztgenannte allerdings nicht. Demgegenüber stagniert die Entwicklung zwischen März und August 2009 über einen längeren Zeitraum. Und nur zwischen November 2009 und Januar 2010 ist einmalig ein leichter Rückgang festzustellen.

*Schaubild 7: Entwicklung der Automatischen Kennzeichenfahndung absolut im zeitlichen Verlauf*

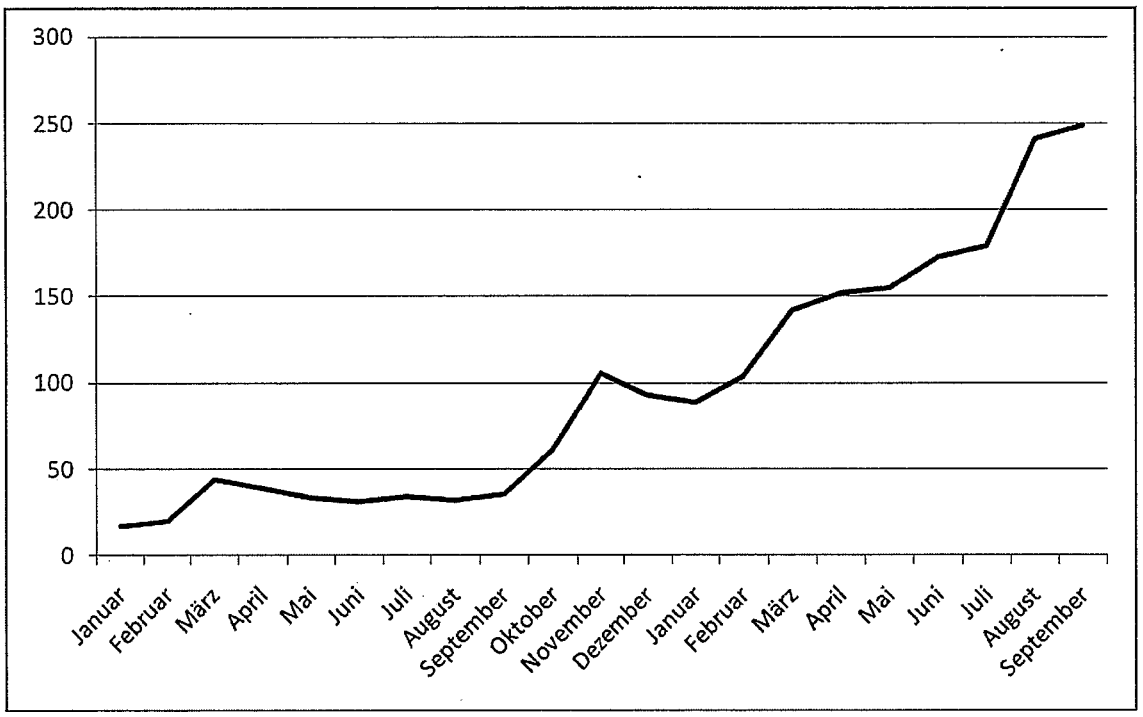


*Tabelle 12: Entwicklung der AKF in Relation zu der Gesamtzahl polizeilicher Einsätze*

| Jahr | Monat | Einsätze AKF | Polizeiliche Einsätze insges.* | % |
|---|---|---|---|---|
| 2009 | Januar | 17 | 18.349 | 0,09 |
| 2009 | Februar | 20 | 17.629 | 0,11 |
| 2009 | März | 44 | 20.587 | 0,21 |
| 2009 | April | 39 | 22.441 | 0,17 |
| 2009 | Mai | 33 | 23.291 | 0,14 |
| 2009 | Juni | 31 | 21.194 | 0,15 |
| 2009 | Juli | 34 | 24.595 | 0,14 |
| 2009 | August | 32 | 24.682 | 0,13 |
| 2009 | September | 35 | 21.476 | 0,16 |
| 2009 | Oktober | 61 | 21.361 | 0,29 |
| 2009 | November | 106 | 20.088 | 0,53 |
| 2009 | Dezember | 93 | 19.891 | 0,47 |
| 2010 | Januar | 89 | 18.119 | 0,49 |
| 2010 | Februar | 104 | 16.294 | 0,64 |
| 2010 | März | 142 | 19.209 | 0,74 |
| 2010 | April | 152 | 19.264 | 0,79 |
| 2010 | Mai | 155 | 21.154 | 0,73 |
| 2010 | Juni | 173 | 19.823 | 0,87 |
| 2010 | Juli | 179 | 22.176 | 0,81 |
| 2010 | August | 241 | 21.271 | 1,13 |
| 2010 | September | 249 | 18.593 | 1,34 |
| **insgesamt** | | **2.029** | **431.487** | **0,47** |

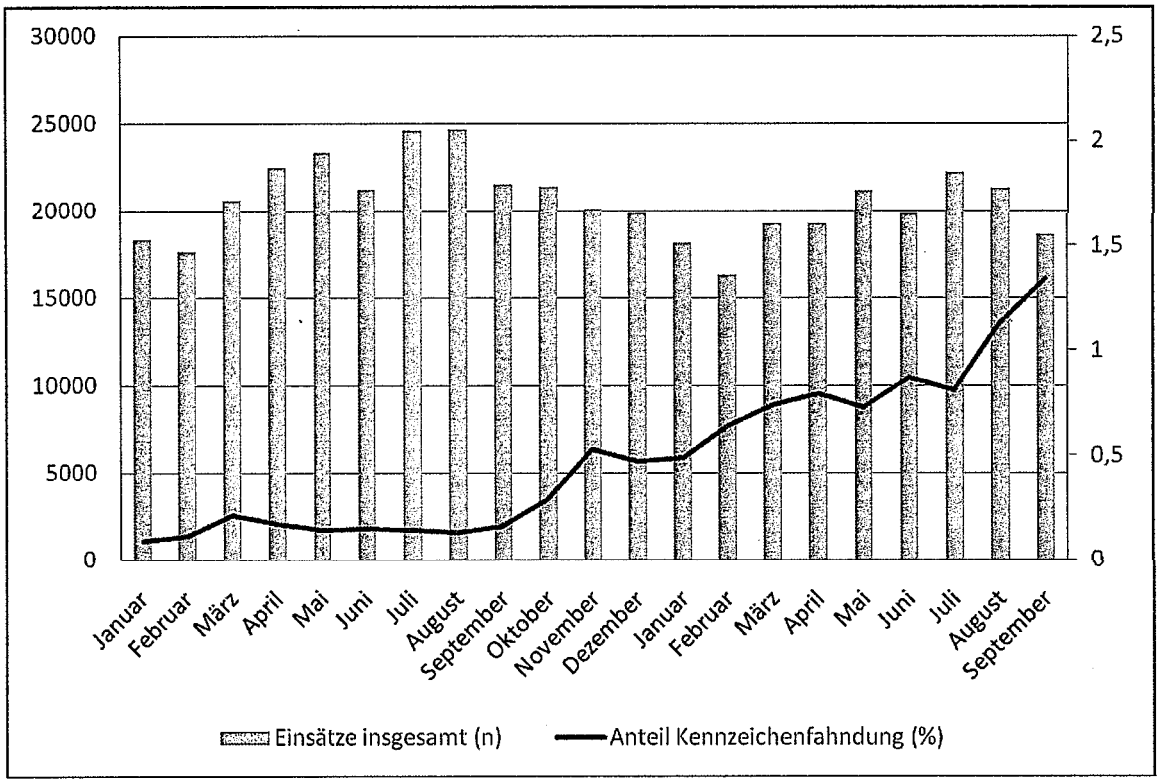
*) Gesamtzahl der Einsätze zur Gefahrenabwehr und Strafverfolgung ohne Verkehrs- und sonstige Einsätze; Basis: ELBOS-Einsatznummern.

Tabelle 12 gibt Auskunft über die Entwicklung der automatischen Kennzeichenfahndung in Relation zu der Gesamtzahl der polizeilichen Einsatzzahlen. Zu den Vergleichswerten aus dem ELBOS-System gilt das oben unter Pkt. 2.1 Gesagte. Wie erwähnt werden hier die repressiven Polizeieinsätze mit berücksichtigt, um der Dominanz der Totalentwendungsfälle Rechnung zu tragen. Wie der Blick auf Schaubild 8 zeigt, ergibt sich auf dieser Basis keine wesentliche Veränderung in dem Grundmuster der monatlichen Schwankungsbreite. Allerdings verändert sich die Bezugsgröße erheblich. Während in dem Untersuchungszeitraum durchschnittlich 14.410 präventive Einsätze monatlich anfielen[304], waren es zusammen mit den repressiven 20.547. Insgesamt waren in den 21 Monaten der Evaluation zusammen 431.487 präventive und repressive Einsätze zu verzeichnen. Dieser Grundgesamtheit steht eine Zahl von insgesamt 2.029 Einsätzen der automatischen Kennzeichenfahndung gegenüber. Das macht im Durchschnitt etwa ein halbes Prozent (0,47 %) aller Maßnahmen aus. Dieser rechnerische Durchschnittswert wird genau im Dezember 2009 erreicht und anschlie-

[304] Vgl. oben Tabelle 3.

ßend dauerhaft und zunehmend überschritten. Das Ausmaß des Anstiegs bei den relativen Anwendungszahlen wird in Schaubild 8 deutlich sichtbar. Er kann anhand verschiedener Rechenexempel noch weiter präzisiert werden. So wurde als Durchschnittswert für das Jahr 2009 ein Anteil von 0,21 % errechnet, für 2010 (Jan. - Sept.) ein Wert von 1,08 %; das ist ein Anstieg um das Vierfache (414 %). Und stellt man dem Ausgangswert aus dem Monat Januar 2009 (0,09 %) den Monatswert für September 2010 gegenüber (1,34 %), so ergibt sich ein Zuwachs um das Vierzehnfache (1.448 %). Die Entwicklung reflektiert im Übrigen auch den Übergang von der Test- und Implementationsphase in den Regelbetrieb.

*Schaubild 8: Entwicklung der Einsatzzahlen und der polizeilichen Einsätze insgesamt**




*) Gesamtzahl der Einsätze zur Gefahrenabwehr und Strafverfolgung ohne Verkehrs- und sonstige Einsätze; Basis: ELBOS-Einsatznummern.

### *3.2 Einsatzart*

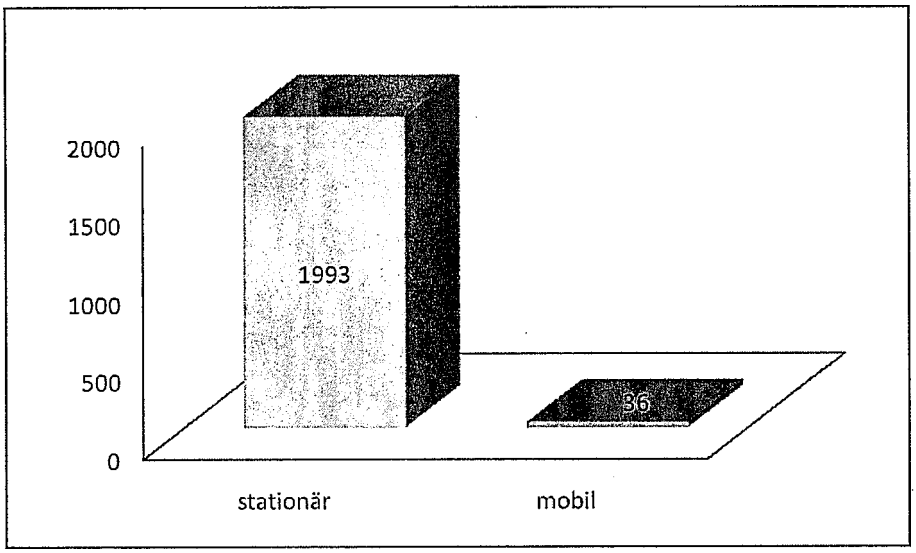
*Tabelle 13: Art der eingesetzten Systeme*

| Einsatzart | Anzahl | % |
|---|---|---|
| stationär | 1.993 | 98.23 |
| mobil | 36 | 1,77 |
| **insgesamt** | **2.029** | **100** |

Der Schwerpunkt hinsichtlich der Art der eingesetzten Systeme liegt ganz eindeutig bei den stationären Anlagen. 98 % aller Einsätze im Untersuchungszeitraum erfolgten durch Aktivie-

rung der jeweiligen Fahndung in den fest installierten Anlagen (n = 1.993), während die mobilen Systeme insgesamt nur 36 Mal zum Einsatz kamen (Tabelle 13 bzw. Schaubild 9). Dies ist neben der Struktur der bearbeiteten Fälle vor allem mit den praktischen Vorteilen der stationären gegenüber den mobilen Anlagen erklärbar. Während die Letzteren mit einem erheblichen logistischen Aufwand verbunden sind – die Anlage muss zum Einsatzort transportiert, aufgebaut, in Betrieb gesetzt und nach Einsatzende abgebaut werden, neben den bedienenden Beamten und den Beamten an der vorgelagerten Kontrollstelle werden mindestens zwei Polizeifahrzeuge temporär gebunden – erfordert der Einsatz der stationären Anlage aufgrund ihrer permanenten Betriebsbereitschaft nur einen sehr kurzen Vorlauf, um eine aktuelle Fahndung durch den Fachkoordinator Kennzeichenfahndung oder sonstige besonders autorisierte Beamte in dem Zentralrechner zu aktivieren.

*Schaubild 9: Art der eingesetzten Systeme (2)*




Gegenwärtig sind in Brandenburg fünf stationäre und drei mobile Systeme im Einsatz. Seit dem Zeitpunkt der Interviews im Oktober 2009[305] wurden zwei weitere stationäre Systeme implementiert. Damit ist, zumindest nach dem damaligen Planungsstand, das Endausbaustadium erreicht. Beide Systemarten haben aus einsatztechnischer Perspektive ihren jeweils eigenen Sinn und sind auf unterschiedliche Einsatzerfordernisse zugeschnitten. Neben möglichen einsatztaktischen Vorteilen, die aus der schnelleren Einsatzfähigkeit und dem auf mehrere Standorte gleichzeitig verteilten Kontrollvorgang resultieren können, kommt der eigentliche ökonomische Mehrwert der automatischen Kennzeichenfahndung im Hinblick auf die Schonung von Personal- und Sachressourcen gegenüber der traditionell durch Polizeibeamte visuell durchgeführten Fahndungsmethode aber gerade bei den stationären Anlagen zum Tragen.

---

305 Vgl. Teil G, Anhang 2.

*Tabelle 14: Einsatzmodus der Systeme*

| Einsatzmodus | Anzahl | % |
|---|---|---|
| Fahndungsmodus | 2.005 | 98,82 |
| Aufzeichnungsmodus | 2 | 0,1 |
| Fahndungs- und Aufzeichnungsmodus | 22 | 1,08 |
| **insgesamt** | **2.029** | **100** |

Ein eindeutiger Schwerpunkt ergibt sich auch bei dem Blick auf den Einsatzmodus der Systeme bei der Durchführung der Maßnahmen. Mehr als 98 % der Einsätze dienten ausschließlich der Fahndung (Tabelle 14). Nur 24 Mal wurde der Aufzeichnungsmodus aktiviert, davon zweimal ausschließlich. Bei diesen Fällen handelte es sich durchweg um längerfristige Observationen, meist im Zusammenhang mit Ermittlungen im Bereich der organisierten Kriminalität. Diese Fälle lagen zumeist in der Zuständigkeit des Landeskriminalamtes, darunter in mehreren Fällen in Amtshilfe für die Berliner Strafverfolgungsbehörden.

### *3.3 Anordnung der Maßnahmen*

Eine größere Vielfalt als im Bereich der Verkehrsdatenabfrage zeigt die Verteilung der anordnenden Behörden. Die richterlichen bzw. staatsanwaltlichen Anordnungen beziehen sich ausschließlich auf den repressiven Einsatz der Maßnahmen, insbesondere im Kontext der längerfristigen Observationen. Das Polizeipräsidium bzw. das Landeskriminalamt zeichnen hingegen zum einen für die präventiven Anwendungen auf der Grundlage von § 36a BbgPolG verantwortlich, zum anderen für die Fahndungen bei den Totalentwendungen, die in Brandenburg, wie bereits ausgeführt, gegenwärtig ausschließlich auf der Grundlage von § 100h Abs. 1 Nr. 2 StPO durchgeführt werden. Beide Rechtsgrundlagen setzen bekanntlich keine richterliche Prüfung und Anordnung voraus.

*Tabelle 15: Anordnung der Maßnahmen**

| Anordnende Behörde | Anzahl | % |
|---|---|---|
| 1. Gericht | 44 | 2,48 |
| 2. StA | 11 | 0,62 |
| 3. LKA | 35 | 1,97 |
| 4. Polizeipräsidium | 1.681 | 94,81 |
| 5. Andere | 2 | 0,11 |
| **insgesamt** | **1.773** | **100** |

*) Missing values: 256 (12,6 %).

Insgesamt wurden fast 97 % aller Einsätze auf der Grundlage einer polizeilichen Anordnung durchgeführt (siehe Tabelle 15, Nummern 3 bis 5), der verbleibende Rest (siehe ebendort, Nummern 1 und 2) nach einer justiziellen Vorentscheidung (Staatsanwaltschaft oder Gericht). Die gegenwärtige Anordnungswirklichkeit mit ihrem Schwerpunkt *polizeilich* angeordneter Strafverfolgungsmaßnahmen mag auf den ersten Blick etwas kurios erscheinen,

ist aber ein Spiegelbild der aktuellen Rechtslage, die die Fahndung nach gestohlenen Fahrzeugen in Brandenburg eben ausschließlich der Strafverfolgung zuordnet.

### *3.4 Anlass und Zielsetzung der Maßnahmen*

Die besondere Fallstruktur der automatischen Kennzeichenfahndung wird bei der Analyse der Anlässe für die durchgeführten Einsätze der automatischen Kennzeichenfahndung besonders evident. Die Fallgestaltungen, die das Einsatzspektrum der Verkehrsdatenabfragen bestimmten, nämlich die Abwehr von Gefahren für Leib oder Leben eines Menschen, spielt bei der Kennzeichenfahndung nur eine nachrangige Rolle und waren in gerade fünf Prozent der Fälle der unmittelbare Anlass der Maßnahme (Tabelle 16). Auch das Spektrum schwerer Straftaten erscheint sehr begrenzt. Fahndungen im Zusammenhang mit Tötungsdelikten waren ebenso auf Einzelfälle beschränkt wie BtM- und andere Delikte. Unter den sonstigen Delikten findet sich übrigens ein Fall, der in der Öffentlichkeit überregionales Interesse gefunden hat: die Fahndung nach den in einem PKW flüchtigen Ausbrechern aus der JVA Aachen.

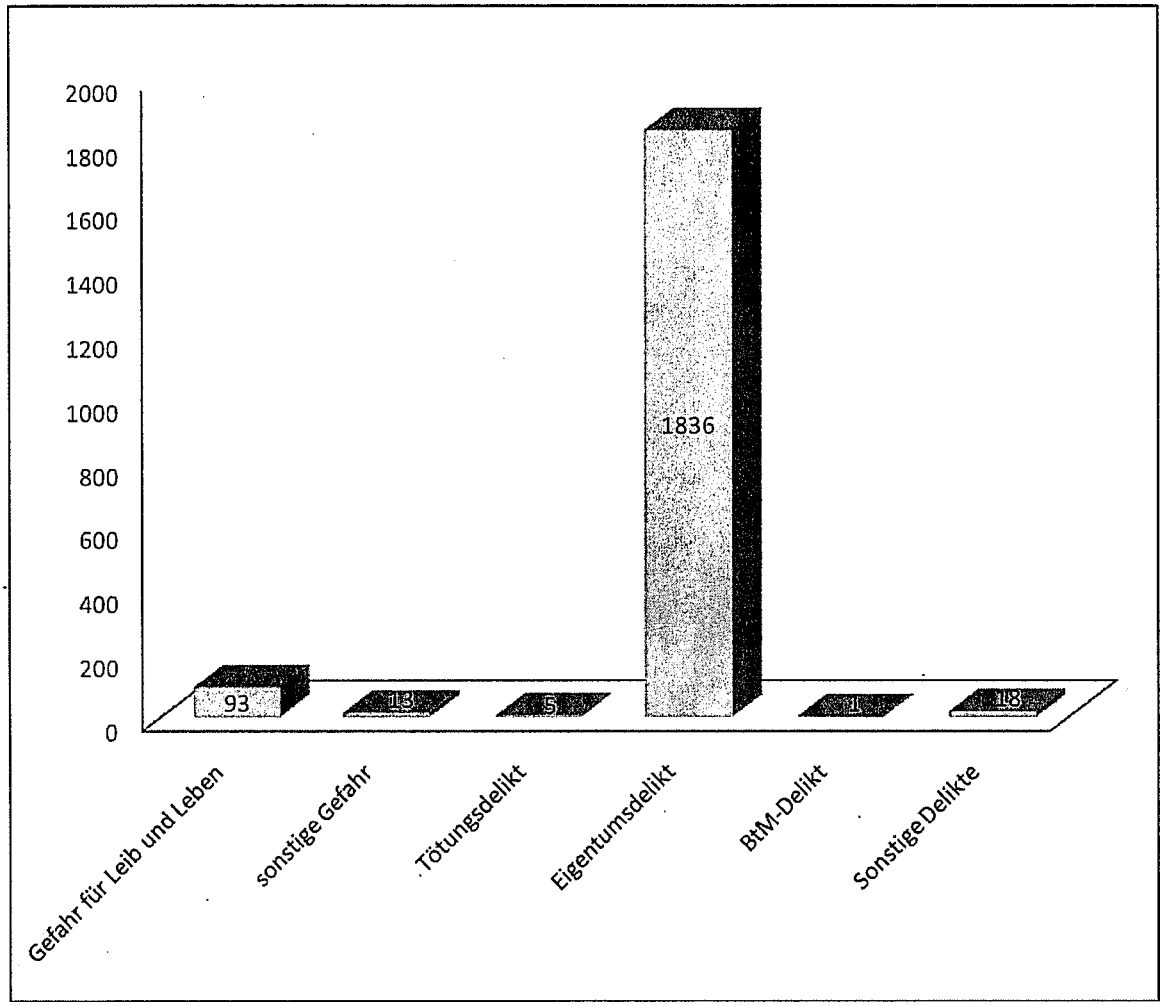
*Tabelle 16: Anlass der Kennzeichenfahndung**

| Anlass | Anzahl | % |
|---|---|---|
| Gefahr für Leib oder Leben | 93 | 4,73 |
| sonstige Gefahr | 13 | 0,66 |
| Tötungsdelikt | 5 | 0,25 |
| Eigentumsdelikt | 1.836 | 93,39 |
| BtM-Delikt | 1 | 0,05 |
| Sonstige Delikte | 18 | 0,92 |
| **insgesamt** | **1.966** | **100** |

*) Missing values: 63 (3,1 %).

Im Wesentlichen geprägt wird die Einsatzwirklichkeit freilich, wie bereits unter Pkt. 3.1 ausgeführt, durch die Totalentwendungsfälle, die hier unter der Rubrik der Eigentumsdelikte erscheinen und deren hauptsächlichen Anteil ausmachen. Mehr als neun von zehn Einsätzen haben einen entsprechenden Hintergrund. Dieses Übergewicht wird in Schaubild 10 auch graphisch sichtbar. Fahndungsgegenstand waren dabei in der großen Mehrzahl der Fälle PKW; aber auch nach anderen Fahrzeugen wurde des Öfteren gesucht. Beispiele aus den Akten waren neben zahlreichen LKW auch Anhänger mit wertvoller Ladung oder ein Trailer mit einer Motor-Yacht (entwendet am Bodensee) und Ähnliches.

*Schaubild 10: Anlass der Kennzeichenfahndung (2)*



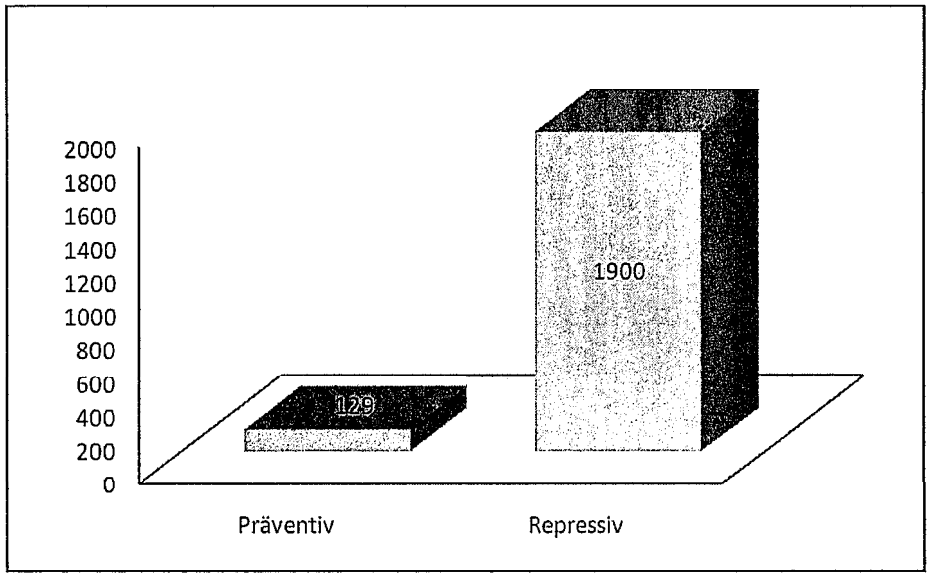

Dieser besondere Schwerpunkt erscheint im Übrigen nicht zufällig, da hier der innere Zusammenhang zu dem Anlass der Maßnahme selbstredend am deutlichsten zu Tage tritt. In allen diesen Fällen ist das amtliche Kennzeichen des Fahndungsobjektes bekannt, und eine zielführende Fahndung muss sich zwangsläufig auf den Straßenraum konzentrieren. Schließlich ist in diesen Fällen meistens auch keine Alternative mit vergleichbarer Erfolgsaussicht ersichtlich. Diese Konzentration auf straßenverkehrsbezogene Vorgänge vermag darüber hinaus zu indizieren, dass die Maßnahme auch nicht in unverhältnismäßigem Umfang in anderen Fällen zum Einsatz kommt.

*Tabelle 17: Zielsetzung der Kennzeichenfahndung*

| Zielsetzung | Anzahl | % |
|---|---|---|
| präventiv | 129 | 6,36 |
| repressiv | 1.900 | 93,64 |
| **insgesamt** | **2.029** | **100** |

Das erwähnte, mit dem besonderen Fallspektrum erklärbare Übergewicht der formal repressiv orientierten Einsätze tritt auch bei der Variablen „Zielsetzung" noch einmal sehr deutlich zutage. Sie wurde auf der Basis der jeweils angegebenen Rechtsgrundlage erstellt. Gut 93 % der Einsätze sind danach dem Bereich der Strafverfolgung zuzuordnen, knapp 6 % der Gefahrenabwehr (Tabelle 17 und Schaubild 11). Diese formale Zuordnung lässt die präventiven Aspekte der Polizeieinsätze bei diesem Delikttypus letztlich nicht erkennen.

*Schaubild 11: Zielsetzung der Kennzeichenfahndung (2)*




### *3.5 Eingriffsbreite der Kennzeichenfahndung*

Wie bei der Verkehrsdatenabfrage soll auch hier besondere Aufmerksamkeit der Analyse der Eingriffsbreite der durchgeführten Maßnahmen gelten. Die Eingriffsbreite wurde im Hinblick auf die automatische Kennzeichenfahndung mit abweichenden Parametern operationalisiert. Sie bestimmt sich in diesem Fall zunächst ganz wesentlich an der Zusammensetzung der zugrundeliegenden Fahndungsdateien. Je nachdem, ob lediglich nach einem individuellen Kennzeichen gefahndet wird oder ob die Fahndungsdatei Hunderte oder gar Tausende von Kennzeichen umfasst, erhöht sich die Trefferwahrscheinlichkeit unmittelbar.

*Tabelle 18: Anzahl überwachter Kfz-Kennzeichen nach Fallgruppen**

| Anzahl Kennzeichen in Fahndung | Häufigkeit | % | Fallgruppen |
|---|---|---|---|
| 0 | 2 | 0,1 | div. |
| 1 | 1.952 | 96,2 | div. |
| 2 | 22 | 1,08 | div. |
| 3 | 5 | 0,24 | div. |
| 4 | 10 | 0,49 | div. |
| 6 | 1 | 0,05 | k.A. |
| 8 | 1 | 0,05 | k.A. |
| 9 | 2 | 0,1 | div. |
| 13 | 1 | 0,05 | sonstiges |
| 15 | 1 | 0,05 | Fußball |
| 17 | 1 | 0,05 | sonstiges |
| 19 | 1 | 0,05 | Fußball |
| 20 | 2 | 0,1 | sonstiges |
| 25 | 1 | 0,05 | k.A. |
| 27 | 1 | 0,05 | Kfz-Diebst. |
| 30 | 1 | 0,05 | Kfz-Diebst. |
| 39 | 3 | 0,14 | Kfz-Diebst. |
| 56 | 1 | 0,05 | Rocker |
| 61 | 2 | 0,1 | Kfz-Diebst. |
| 65 | 1 | 0,05 | Rocker |
| 87 | 1 | 0,05 | Kfz-Diebst. |
| 108 | 1 | 0,05 | Kfz-Diebst. |
| 157 | 2 | 0,1 | Kfz-Diebst. |
| 159 | 1 | 0,05 | Kfz-Diebst. |
| 352 | 1 | 0,05 | Rocker |
| 1.139 | 1 | 0,05 | Rocker |
| 1.162 | 2 | 0,1 | Rocker |
| 1.205 | 1 | 0,05 | Rocker |
| 1.245 | 1 | 0,05 | Rocker |
| 1.314 | 2 | 0,1 | Rocker |
| 1.498 | 1 | 0,05 | Rocker |
| 1.521 | 1 | 0,05 | Rocker |
| 2.425 | 1 | 0,05 | Rocker |
| 3.615 | 1 | 0,05 | Rocker |
| 4.192 | 1 | 0,05 | Fußball |
| **insgesamt** | **2.029** | **100** | |

*) Durchschittswerte: 12,53 (mean) bzw. 1 (median).

Tabelle 18 gibt Auskunft über die genaue Anzahl von Kennzeichen, nach denen bei den einzelnen Maßnahmen jeweils gefahndet wurde. Den Kategorien wurden ergänzend die dazugehörigen Fallgruppen zugeordnet. Dabei werden mehrere Punkte erkennbar, die den Einsatz-

alltag in Brandenburg charakterisieren und über den Zeitverlauf hinweg auch stabil bleiben. Zunächst fällt die große Varianz verschiedener Größenordnungen auf, die – mit Ausnahme der Individualfahndung – meist nur ein- oder zweimal vorkommen. Dies belegt die Aussage der befragten Praktiker, dass bei den Einsätzen nicht pauschal auf vorhandene Gefährder- und Fahndungsdateien von BKA, INTERPOL oder anderen Dienststellen zurückgegriffen wird, sondern dass tatsächlich für jeden Fall ad hoc eine individuelle Liste mit den jeweils relevant erscheinenden Kennzeichen zusammengestellt wird.

Erkennbar wird sodann, dass es eine beschränkte Zahl von Einsätzen gibt, bei denen sehr viele, teilweise mehrere Tausend Kennzeichen in den aktuellen Fahndungsbestand eingehen. Diesen liegen fast ausschließlich Ereignisse im Zusammenhang mit der Rockerszene zugrunde. Anlässe sind entweder konkrete Fälle krimineller Aktivitäten der Szene oder einzelne Veranstaltungen wie bspw. eine sog. „Jack Daniels Night" oder ein „Memory Run" des Bandidos MC, die Gründungsfeier, die Geburtstagsfeier oder ein „City Run" der konkurrierenden Hells Angels (HAMC) bzw. ein als „Rockerhochzeit" vermerktes Ereignis, die unter dem Gesichtspunkt der Gefahrenabwehr beobachtet wurden.

Als weiterer Schwerpunkt fallen die Einsätze im Zusammenhang mit Fußballspielen auf. In diesem Bereich gab es zum einen mehrere Fahndungen gegen jeweils etwa ein Dutzend namentlich bekannter Personen aus der Gruppe der Gewalttäter im Zusammenhang mit Sportereignissen, die aus Anlass von Spielen des FC Energie Cottbus durchgeführt wurden. Zum anderen gab es einen einzelnen Einsatz bei einem bestimmten Spiel zwischen Hertha BSC und wiederum dem FC Energie Cottbus, bei dem die Höchstzahl von 4.129 Datensätzen eingespeist war. Auch zu dem Bereich der fußballbezogenen Einsätze ist hervorzuheben, dass die brandenburgische Polizei die Anlassbezogenheit streng beachtet und bei der Vorbereitung jeweils eine aktuelle Fahndungsdatei aufbereitet und nicht etwa pauschal auf die Datei „Gewalttäter Sport" des BKA zurückgreift. Damit ist die Gefahr von Fehltreffern bei Personen, die in keinerlei Verbindung zu den beiden Vereinen des aktuell beobachteten Spiels stehen, die zu der fraglichen Zeit aber rein zufällig in Brandenburg unterwegs sein könnten, so gut wie ausgeschlossen.

Neben diversen anderen straftatbezogenen Fahndungen, die beispielsweise Fälle illegalen Zigarettenschmuggels aus Polen, Erpressungen, Überfälle auf Geldinstitute und ein Tötungsdelikt mit anschließender Flucht zum Anlass hatten, können schließlich zwei verschiedene Fallgruppen des Kfz-Diebstahls unterschieden werden, die jeweils ein typisches Fahndungsmuster aufweisen. Auf der einen Seite stehen dabei bandenmäßige Kfz-Diebstähle, meist im Kontext der organisierten Kriminalität; die Fahndungsstrategie besteht hier in der Suche nach allen bekannten Kennzeichen tatverdächtiger Personen aus dem Umfeld einer verdächtigen Gruppe, die bei einer mutmaßlichen Überführung als Voraus- oder Begleitfahrzeuge in Erscheinung treten könnten, sowie, soweit bereits bekannt, das oder die Kennzeichen gerade entwendeter Fahrzeuge. Diese Fälle dominieren den mittleren Bereich in Tabelle 18; sie können wenige Dutzend, teilweise aber auch mehr als hundert Kennzeichen betreffen. Auf der anderen Seite steht die „klassische" Totalentwendung individueller Fahrzeuge. In diesen Fällen gibt es zumeist keine weiteren Erkenntnisse zum Tathintergrund, sodass sich die polizei-

lichen (Sofort-)Maßnahmen auf die möglichst umgehende Eingabe des jeweiligen Kennzeichens in das AKF-System beschränken (müssen), in der Hoffnung, dass das betreffende Fahrzeug sich noch im brandenburgischen Straßenraum bewegt. Diese Einzelfahndungen machen mit einem Anteil von 96 % den Hauptanteil der Maßnahmen aus.

Die Nullvariante in der ersten Tabellenzeile steht schließlich für die beiden Fälle, in denen ausschließlich der Aufzeichnungsmodus zum Einsatz kam[306]. Hier wurde effektiv nach keinen konkreten Kennzeichen gefahndet.

Die besondere Verteilung der Fälle führt auch zu deutlichen Unterschieden bei den Mittelwerten. Einerseits ergibt sich unter Berücksichtigung der Fälle, in denen sehr viele Kennzeichen eingelesen wurden, ein (fiktiver) Wert von durchschnittlich 12,5 Kennzeichen pro Maßnahme. Anders als dieser arithmetische Mittelwert (mean) berücksichtigt der Median die tatsächliche Verteilungshäufigkeit der verschiedenen Ausprägungen und gibt somit den Zentralwert an. Dieser muss bei einer so ungleichen Verteilung wie hier maßgeblich zur Interpretation herangezogen werden. Er liegt bei 1. Damit bestätigt sich auch statistisch, dass die Einsatzwirklichkeit der automatischen Kennzeichenfahndung in Brandenburg entscheidend geprägt wird durch die Fälle, in denen jeweils gezielt nach nur einem einzelnen Kennzeichen gefahndet wird. Diese Fälle tragen auch die allgemeine Zunahme in der Anwendungshäufigkeit ganz wesentlich mit. Dass diese Fallkonstellation so dominierend ist, mag, neben dem bereits erwähnten engen Bezug dieser Deliktsart zum Straßenverkehr, vor allem in der Zunahme des Kfz-Diebstahls[307] erklärbar sein. Im Übrigen geht mit dem Übergang der Kennzeichenfahndung von der Test- und Implementationsphase in den Regelbetrieb ein routinierterer Einsatz der Maßnahme einher. Im Gegensatz zu diesem Regelanwendungsfall fallen die Einsätze mit umfangreichen Suchdateien (Fußball, Rocker) zwar eher auf – und nehmen in der obigen Tabelle auch optisch größeren Raum ein –, stellen auf das Ganze betrachtet aber Ausnahmekonstellationen dar, die statistisch, wie aufgezeigt, nicht ins Gewicht fallen.

*Tabelle 19: Anzahl eingesetzter Systeme**

| Anzahl eingesetzter Systeme | Einsatz-häufigkeit |
|---|---|
| 1 | 251 |
| 2 | 61 |
| 3 | 171 |
| 4 | 402 |
| 5 | 1.140 |
| **insgesamt** | **2.025** |

*) Missing values: 4 (0,2 %).

Ein weiterer Faktor, der eine wesentliche Rolle für die Beurteilung der Eingriffsbreite spielt, ist die Anzahl der Systeme, die bei einer Fahndung zum Einsatz kommen. Man könnte inso-

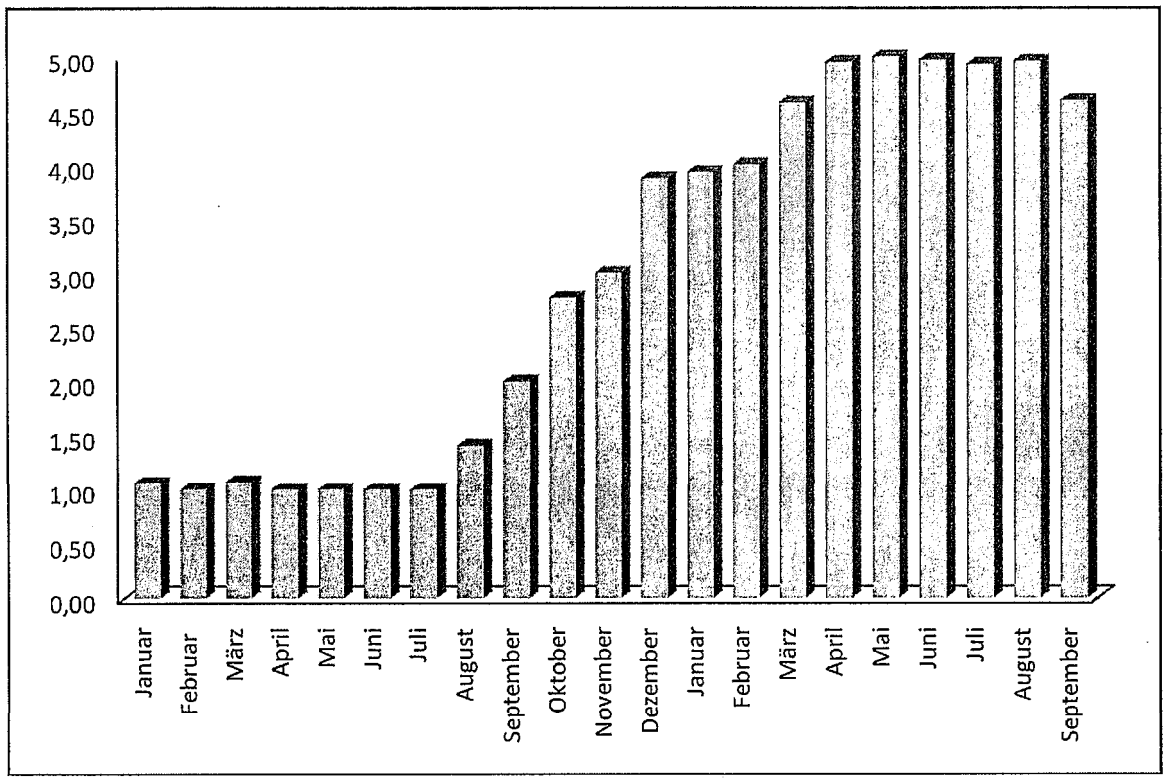
306 Vgl. oben Tabelle 14.

307 Vgl. hierzu die Ausführungen in Teil D, Pkt. 3.

weit auch von der Einsatz- bzw. Überwachungsdichte sprechen. Hier würde die Wirkung potenziert, wenn statt eines einzelnen oder nur wenigen Systemen etwa eine Vielzahl über das Land verteilter Anlagen oder als Extrembeispiel sogar die Gesamtheit der Überwachungsbrücken für die LKW-Maut zum Einsatz käme. Je nachdem kann entweder von einer punktuellen oder einer flächendeckenden Überwachung gesprochen werden, wobei die letztere Variante unter Zugrundelegung der bislang vom BVerfG zu Fragen der automatischen Kennzeichenfahndung veröffentlichten Grundsätze sicherlich als unverhältnismäßig einzustufen wäre[308].

Wie sich aus Tabelle 19 ergibt, kommen inzwischen bei der Mehrzahl der Einsätze fünf Systeme zum Einsatz. Dies ist im Hinblick auf die Fallstruktur plausibel; denn bei den individuellen Fahndungen im Fall der Totalentwendung werden in der Regel die aktuell fünf stationären Anlagen aktiviert. Bevor die Endausbaustufe erreicht war, waren die entsprechenden Fahndungen auf die seinerzeit verfügbaren drei bzw. vier fest installierten Anlagen beschränkt. Der Einsatz eines einzelnen oder zweier Systeme betrifft hingegen zumeist die mobilen Einsätze. Diese verteilen sich über den gesamten Evaluationszeitraum hinweg. Das belegt, dass bei punktuellen, auf einen bestimmten geographischen Einsatzraum begrenzten mobilen Maßnahmen nicht quasi automatisch die stationären Anlagen mit aktiviert werden.

*Schaubild 12: Durchschnittliche Anzahl eingesetzter Systeme im Zeitverlauf*




308 Vgl. hierzu die rechtlichen Ausführungen in Teil D, Pkt. 3.

In Schaubild 12 wird ergänzend die zeitliche Entwicklung der Einsatzdichte nachgezeichnet. Während bis zur Jahresmitte 2009 im Durchschnitt stets nur ein System zum Einsatz kam, erhöhte sich deren Anzahl dann im zweiten Halbjahr 2009 parallel zu dem weiteren Ausbau zügig auf zwei bzw. drei Systeme. Im Jahr 2010 erfolgte der Regeleinsatz zunächst mit vier, seit April dann mit fünf Anlagen. Im März und September 2010 scheint eines der stationären Systeme zeitweilig nicht verfügbar gewesen zu sein. Dies sind freilich Durchschnittswerte. In Einzelfällen kamen jeweils auch weniger Systeme zum Einsatz, insbesondere bei den erwähnten mobilen Einsätzen. Die exakten Monatswerte, auf denen Schaubild 13 basiert, sind in Tabelle 20 nachgewiesen.

*Tabelle 20: Durchschnittliche Anzahl eingesetzter Systeme*

| Jahr | Monat | Durchschnittliche Anzahl eingesetzter Systeme |
|---|---|---|
| 2009 | Januar | 1,06 |
| 2009 | Februar | 1,00 |
| 2009 | März | 1,07 |
| 2009 | April | 1,00 |
| 2009 | Mai | 1,00 |
| 2009 | Juni | 1,00 |
| 2009 | Juli | 1,00 |
| 2009 | August | 1,41 |
| 2009 | September | 2,00 |
| 2009 | Oktober | 2,77 |
| 2009 | November | 3,00 |
| 2009 | Dezember | 3,87 |
| 2010 | Januar | 3,93 |
| 2010 | Februar | 4,00 |
| 2010 | März | 4,57 |
| 2010 | April | 4,95 |
| 2010 | Mai | 5,00 |
| 2010 | Juni | 4,97 |
| 2010 | Juli | 4,93 |
| 2010 | August | 4,96 |
| 2010 | September | 4,59 |

Ein weiteres Merkmal, das die Eingriffsbreite mit bestimmt, betrifft die Dauer der Einsätze. Je nachdem, ob eine Fahndungsmaßnahme eine Stunde oder einen Monat andauert, verändert sich die Wahrscheinlichkeit, von der Fahndungsmaßnahme erfasst zu werden, ebenfalls. Für die große Mehrzahl aller Fälle waren auch hierzu Angaben vorhanden. Sie sind im Einzelnen in Tabelle 21 ausgewiesen.

Aus der Verteilung lassen sich unter dem zeitlichem Aspekt – von Einzelfällen abgesehen, die quantitativ jeweils nicht ins Gewicht fallen und zum großen Teil wiederum die mobilen

Einsätze betreffen – grob drei unterschiedliche Einsatzmuster identifizieren. Zum Ersten gibt es Fahndungsmaßnahmen, die auf eine oder einige wenige Stunden begrenzt sind. Auch die Fälle, die etwas länger als einen halben Tag (bzw. die Nacht über) dauern, können dieser Gruppe zugeordnet werden. Sie erreicht zusammen eine Größenordnung von etwa 12 %. Hiervon sind diejenigen Maßnahmen zu unterscheiden, die sich über einen Zeitraum von mehreren Tagen und Wochen erstrecken. In einigen wenigen Fällen zieht sich der Einsatz sogar über mehrere Monate hin. In dieser Gruppe finden sich die Fälle langfristiger Observationen. Sie machen zusammen freilich nicht mehr als etwa 2,5 % aus. Als dritte Gruppe stechen schließlich auch hier wieder die Eilfahndungen in den Totalentwendungsfällen hervor. Die Fahndung nach den jeweiligen Kennzeichen wird hier aus Verhältnismäßigkeitsgründen generell zeitlich befristet[309]. Die vordefinierte Dauer beträgt in diesen Fällen dann exakt 23:59 Std., es sei denn, die Nummer wird vorzeitig wieder gelöscht, beispielsweise im Trefferfall. Dies erklärt, warum die Anzahl dieser Fälle hier etwas niedriger ausfällt als in Tabelle 18.

*Tabelle 21: Dauer der Fahndungsmaßnahmen**

| Dauer | Anzahl | % |
|---|---|---|
| < 1 Std. | 72 | 3,64 |
| < 2 Std. | 25 | 1,26 |
| < 3 Std. | 25 | 1,26 |
| < 4 Std. | 15 | 0,76 |
| < 5 Std. | 18 | 0,91 |
| < 6 Std. | 11 | 0,56 |
| < 7 Std. | 14 | 0,71 |
| < 8 Std. | 5 | 0,25 |
| < 9 Std. | 2 | 0,10 |
| < 10 Std. | 3 | 0,15 |
| < 11 Std. | 0 | 0,00 |
| < 12 Std. | 1 | 0,05 |
| 12 - 23 Std. | 39 | 1,97 |
| 23 - 24 Std. | 1.700 | 85,86 |
| 1 - 3 Tage | 29 | 1,46 |
| 3 Tage - 1 Monat | 6 | 0,30 |
| bis 2 Monate | 5 | 0,25 |
| bis 3 Monate | 9 | 0,45 |
| bis 4 Monate | 1 | 0,05 |
| **insgesamt** | **1.980** | **100** |

*) Missing values: 49 (2,4 %).

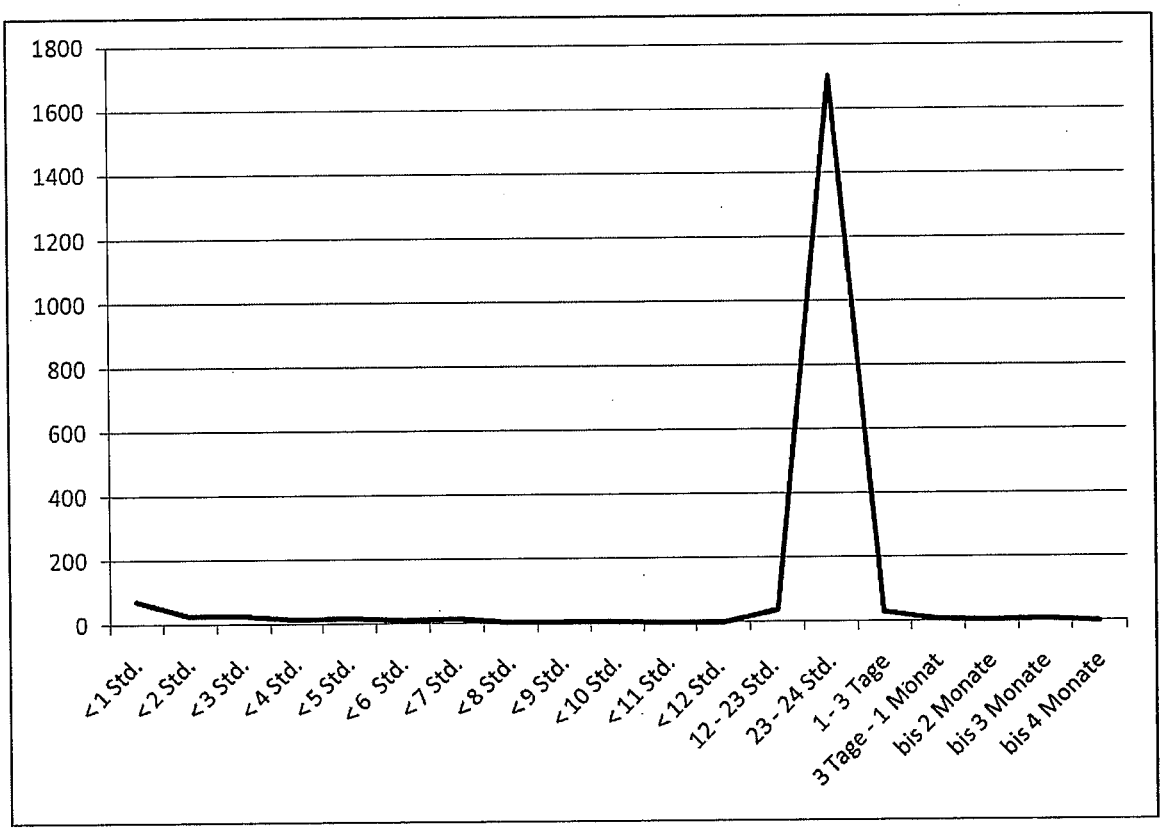
Wie sehr diese Eilfahndungen die Einsatzwirklichkeit in Brandenburg auch unter dem Gesichtspunkt der Einsatzdauer prägen, wird in Schaubild 13 besonders anschaulich. Für die

---

309 Rahmenrichtlinie zur automatischen Kennzeichenfahndung, Ziff. 4.2 (a).

Gesamtbewertung kann die Situation daher dahingehend zusammengefasst werden, dass die Maßnahmen in der Regel die Dauer von 24 Stunden nicht überschreiten.

*Schaubild 13: Dauer der Fahndungsmaßnahmen*




### *3.6 Erfolg der Maßnahmen (Treffer)*

Abschließend wurde der Erfolg der Maßnahmen analysiert, konkret bezogen auf das Primärziel der automatischen Kennzeichenfahndung: die Treffer. Entsprechende Angaben waren zu allen 2.029 Fällen zu erhalten. Die Ergebnisse sind in Tabelle 22 aufbereitet. Auch hier sind wieder die dazugehörigen Fallgruppen ausgewiesen. Zunächst wird deutlich, dass die Trefferquote insgesamt gering ist. Nur in 2,62 % der Fälle kam es zu einer positiven Treffermeldung. Den höchsten Anteil haben dabei, im Hinblick auf die große Zahl der Fälle wenig überraschend, die Eilfahndungen. Auf sie entfällt gut die Hälfte der erfolgreichen Maßnahmen. Aber auch die Suche nach einer suizidgefährdeten Person sowie den nach dem erwähnten Tötungsdelikt mit einem Kind flüchtigen Tatverdächtigen war erfolgreich. Des Weiteren konnten u.a. ein Waffendiebstahl verhindert und der Tatverdächtige eines Bandendiebstahls festgenommen werden. Höhere Trefferquoten wurden dann, auch das ist erwartungsgemäß, auf der Grundlage der umfangreicheren Fahndungsdateien bzw. der längerfristigen Einsätze erzielt. Im letzteren Fall waren es mitunter eines oder mehrere observierte Fahrzeuge, die die Anlage jeweils mehrfach passierten. Dabei gab es in Einzelfällen Situationen mit einem oder mehreren Dutzend Treffern. Hierunter finden sich vor allem die Fälle organisierter oder ban-

denmäßiger Kriminalität, insbes. bandenmäßige Kfz-Verschiebung und Zigarettenschmuggel. Die höchste Trefferquote findet sich schließlich bei den fußballbezogenen Einsätzen. Hier kam es teilweise zu mehreren Hundert Treffermeldungen. Der Fall in der letzten Tabellenzeile betraf den Einsatz bei einem Fußballspiel zwischen dem FC Energie Cottbus und Hertha BSC, bei dem 4.192 Kennzeichen eingespielt waren (vgl. oben Tabelle 18). Das entspricht einer Trefferquote von 11,5 %.

*Tabelle 22: Treffermeldungen*

| Trefferanzahl | Häufigkeit | % | Fallgruppen |
|---|---|---|---|
| 0 | 1.975 | 97,33 | |
| 1 | 28 | 1,38 | div. |
| 2 | 9 | 0,44 | div. |
| 3 | 1 | 0,05 | Rocker |
| 4 | 1 | 0,05 | Rocker |
| 6 | 1 | 0,05 | Rocker |
| 7 | 1 | 0,05 | sonstiges |
| 8 | 1 | 0,05 | k.A. |
| 11 | 1 | 0,05 | sonstiges |
| 13 | 2 | 0,10 | Kfz-Diebst. |
| 19 | 1 | 0,05 | Kfz-Diebst. |
| 20 | 1 | 0,05 | Rocker |
| 34 | 1 | 0,05 | Kfz-Diebst. |
| 36 | 1 | 0,05 | sonstiges |
| 61 | 1 | 0,05 | Fußball |
| 84 | 1 | 0,05 | Fußball |
| 306 | 1 | 0,05 | sonstiges |
| 391 | 1 | 0,05 | Fußball |
| 483 | 1 | 0,05 | Fußball |
| **insgesamt** | **2.029** | **100** | |

Weitere Folgemaßnahmen, insbesondere mögliche strafrechtliche Konsequenzen für die Betroffenen, konnten auf der Basis der verfügbaren Unterlagen nicht in hinreichender Anzahl erkannt werden. Diese sollten nach dem ursprünglichen Forschungsplan eigentlich ebenfalls erhoben werden, um noch weitere Aussagen zu der Eingriffstiefe der Maßnahmen für die individuell betroffenen Personen treffen zu können. Dieser ergänzende Punkt muss mithin offen bleiben.

### *3.7 Gesamtbilanz der Überwachungssituation in Brandenburg während des Evaluationszeitraumes im Hinblick auf die automatische Kennzeichenfahndung*

Abschließend wurde auch hier eine tagesgenaue Gesamtbilanz der Überwachungssituation, und zwar im Hinblick auf die anlassbezogene automatische Kennzeichenfahndung gem. § 36a BbgPolG, für den Evaluationszeitraum zusammengestellt. Das Ergebnis ist in Tabelle 24 in Kalenderform dargestellt.

*Tabelle 23: Aktiver Fahndungsbestand bei der AKF in Brandenburg für jeden Tag des Evaluationszeitraumes*

| 2009 | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Januar** | **Montag** | **Dienstag** | **Mittwoch** | **Donnerstag** | **Freitag** | **Samstag** | **Sonntag** |
| KW 1 | | | | 0 | 0 | 1 | 2 |
| KW 2 | 1 | 0 | 1 | 1 | 1 | 3.615 | 0 |
| KW 3 | 0 | 0 | 2 | 3 | 4 | 2 | 0 |
| KW 4 | 1 | 0 | 0 | 0 | 2 | 2 | 0 |
| KW 5 | 0 | 1 | 1 | 1 | 1 | 0 | |
| **Febuar** | **Montag** | **Dienstag** | **Mittwoch** | **Donnerstag** | **Freitag** | **Samstag** | **Sonntag** |
| KW 5 | | | | | | | 0 |
| KW 6 | 0 | 0 | 2 | 3 | 6 | 10 | 5 |
| KW 7 | 2 | 3 | 1 | 0 | 0 | 0 | 0 |
| KW 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| KW 9 | 0 | 0 | 0 | 1 | 3 | 2 | |
| **März** | **Montag** | **Dienstag** | **Mittwoch** | **Donnerstag** | **Freitag** | **Samstag** | **Sonntag** |
| KW 9 | | | | | | | 2 |
| KW 10 | 2 | 2 | 1 | 2 | 1.143 | 4.194 | 0 |
| KW 11 | 2 | 3 | 1 | 0 | 1 | 3 | 4 |
| KW 12 | 6 | 5 | 1 | 0 | 3 | 2 | 0 |
| KW 13 | 0 | 0 | 2 | 7 | 5 | 1.246 | 1 |
| KW 14 | 0 | 2 | | | | | |
| **April** | **Montag** | **Dienstag** | **Mittwoch** | **Donnerstag** | **Freitag** | **Samstag** | **Sonntag** |
| KW 14 | | | 2 | 0 | 1 | 4 | 4 |
| KW 15 | 4 | 4 | 4 | 4 | 2 | 0 | 2 |
| KW 16 | 2 | 0 | 1 | 1 | 5 | 6 | 2 |
| KW 17 | 2 | 1 | 2 | 1 | 2.630 | 2.630 | 1 |
| KW 18 | 1 | 0 | 2 | 3 | | | |
| **Mai** | **Montag** | **Dienstag** | **Mittwoch** | **Donnerstag** | **Freitag** | **Samstag** | **Sonntag** |
| KW 18 | | | | | 2 | 2 | 2 |
| KW 19 | 0 | 3 | 3 | 3 | 3 | 3 | 3 |
| KW 20 | 2 | 3 | 3 | 3 | 1 | 0 | 0 |
| KW 21 | 1 | 3 | 2 | 0 | 2 | 3 | 1 |
| KW 22 | 0 | 0 | 0 | 3 | 3 | 2 | 1 |
| **Juni** | **Montag** | **Dienstag** | **Mittwoch** | **Donnerstag** | **Freitag** | **Samstag** | **Sonntag** |
| KW 23 | 0 | 2 | 8 | 10 | 1 | 0 | 1 |
| KW 24 | 3 | 1 | 2 | 4 | 6 | 4 | 0 |
| KW 25 | 0 | 0 | 0 | 2 | 2 | 3 | 1 |
| KW 26 | 2 | 2 | 0 | 0 | 0 | 0 | 0 |
| KW 27 | 0 | 1 | | | | | |

| Juli | Montag | Dienstag | Mittwoch | Donnerstag | Freitag | Samstag | Sonntag |
|---|---|---|---|---|---|---|---|
| KW 27 | | | 0 | 1 | 4 | 4 | 2 |
| KW 28 | 1 | 3 | 2 | 2 | 2 | 2 | 2 |
| KW 29 | 1 | 2 | 3 | 2 | 1 | 0 | 1 |
| KW 30 | 1 | 0 | 0 | 1 | 3 | 5 | 5 |
| KW 31 | 2 | 2 | 1 | 2 | 2 | | |

| August | Montag | Dienstag | Mittwoch | Donnerstag | Freitag | Samstag | Sonntag |
|---|---|---|---|---|---|---|---|
| KW 31 | | | | | | 1 | 0 |
| KW 32 | 0 | 0 | 2 | 1 | 0 | 0 | 1 |
| KW 33 | 3 | 2 | 1 | 2 | 5 | 5 | 1 |
| KW 34 | 0 | 3 | 3 | 1 | 1 | 1 | 2 |
| KW 35 | 3 | 1 | 2 | 3 | 2 | 5 | 5 |
| KW 36 | 3 | | | | | | |

| September | Montag | Dienstag | Mittwoch | Donnerstag | Freitag | Samstag | Sonntag |
|---|---|---|---|---|---|---|---|
| KW 36 | | 1 | 1 | 0 | 0 | 0 | 2 |
| KW 37 | 1 | 2 | 3 | 1 | 3 | 3 | 1 |
| KW 38 | 5 | 5 | 2 | 5 | 4 | 2 | 1 |
| KW 39 | 0 | 1 | 2 | 4 | 3 | 0 | 4 |
| KW 40 | 3 | 2 | 2 | | | | |

| Oktober | Montag | Dienstag | Mittwoch | Donnerstag | Freitag | Samstag | Sonntag |
|---|---|---|---|---|---|---|---|
| KW 40 | | | | 1 | 3 | 2 | 0 |
| KW 41 | 1 | 0 | 0 | 0 | 2 | 3 | 4 |
| KW 42 | 3 | 0 | 0 | 4 | 8 | 9 | 6 |
| KW 43 | 6 | 2 | 4 | 8 | 4 | 5 | 6 |
| KW 44 | 5 | 9 | 9 | 6 | 3 | 1 | |

| November | Montag | Dienstag | Mittwoch | Donnerstag | Freitag | Samstag | Sonntag |
|---|---|---|---|---|---|---|---|
| KW 44 | | | | | | | 1 |
| KW 45 | 2 | 6 | 5 | 12 | 18 | 8 | 4 |
| KW 46 | 3 | 7 | 11 | 9 | 6 | 5 | 2 |
| KW 47 | 4 | 6 | 6 | 8 | 6 | 5 | 5 |
| KW 48 | 6 | 4 | 6 | 10 | 9 | 12 | 8 |
| KW 49 | 2 | | | | | | |

| Dezember | Montag | Dienstag | Mittwoch | Donnerstag | Freitag | Samstag | Sonntag |
|---|---|---|---|---|---|---|---|
| KW 49 | | 11 | 14 | 8 | 5 | 5 | 4 |
| KW 50 | 7 | 12 | 12 | 8 | 8 | 6 | 3 |
| KW 51 | 4 | 7 | 9 | 6 | 5 | 2 | 1 |
| KW 52 | 2 | 2 | 5 | 3 | 2 | 1 | 2 |
| KW 53 | 3 | 4 | 1 | 4 | | | |

| 2010 |
|---|

| Januar | Montag | Dienstag | Mittwoch | Donnerstag | Freitag | Samstag | Sonntag |
|---|---|---|---|---|---|---|---|
| KW 53 | | | | | 3 | 2 | 4 |
| KW 1 | 3 | 1 | 3 | 6 | 4 | 3 | 3 |
| KW 2 | 3 | 5 | 5 | 5 | 358 | 360 | 6 |
| KW 3 | 14 | 11 | 14 | 12 | 6 | 5 | 2 |
| KW 4 | 5 | 7 | 7 | 7 | 9 | 6 | 3 |

| Febuar | Montag | Dienstag | Mittwoch | Donnerstag | Freitag | Samstag | Sonntag |
|---|---|---|---|---|---|---|---|
| KW 5 | 1 | 6 | 7 | 5 | 5 | 2 | 1 |
| KW 6 | 3 | 6 | 9 | 14 | 11 | 4 | 1 |
| KW 7 | 23 | 29 | 14 | 9 | 7 | 6 | 6 |
| KW 8 | 8 | 10 | 12 | 10 | 9 | 8 | 6 |

| März | Montag | Dienstag | Mittwoch | Donnerstag | Freitag | Samstag | Sonntag |
|---|---|---|---|---|---|---|---|
| KW 9 | 11 | 13 | 8 | 6 | 11 | 12 | 3 |
| KW 10 | 4 | 6 | 10 | 16 | 9 | 9 | 7 |
| KW 11 | 6 | 5 | 8 | 6 | 10 | 10 | 5 |
| KW 12 | 6 | 4 | 7 | 18 | 12 | 7 | 6 |
| KW 13 | 7 | 12 | 11 | | | | |

| April | Montag | Dienstag | Mittwoch | Donnerstag | Freitag | Samstag | Sonntag |
|---|---|---|---|---|---|---|---|
| KW 13 | | | | 10 | 7 | 2 | 0 |
| KW 14 | 0 | 0 | 1 | 6 | 6 | 21 | 24 |
| KW 15 | 14 | 14 | 10 | 1.216 | 15 | 15 | 7 |
| KW 16 | 7 | 13 | 11 | 11 | 19 | 16 | 7 |
| KW 17 | 7 | 7 | 7 | 4 | 16 | | |

| Mai | Montag | Dienstag | Mittwoch | Donnerstag | Freitag | Samstag | Sonntag |
|---|---|---|---|---|---|---|---|
| KW 17 | | | | | | 10 | 4 |
| KW 18 | 7 | 12 | 14 | 13 | 16 | 13 | 5 |
| KW 19 | 1 | 3 | 10 | 7 | 8 | 7 | 4 |
| KW 20 | 9 | 11 | 13 | 16 | 10 | 12 | 8 |
| KW 21 | 5 | 11 | 19 | 16 | 7 | 6 | 9 |
| KW 22 | 11 | | | | | | |

| Juni | Montag | Dienstag | Mittwoch | Donnerstag | Freitag | Samstag | Sonntag |
|---|---|---|---|---|---|---|---|
| KW 22 | | 11 | 16 | 20 | 12 | 5 | 4 |
| KW 23 | 7 | 11 | 9 | 9 | 11 | 7 | 4 |
| KW 24 | 9 | 15 | 19 | 20 | 25 | 18 | 8 |
| KW 25 | 10 | 7 | 8 | 11 | 10 | 12 | 10 |
| KW 26 | 8 | 11 | 10 | | | | |

| Juli | Montag | Dienstag | Mittwoch | Donnerstag | Freitag | Samstag | Sonntag |
|---|---|---|---|---|---|---|---|
| KW 26 | | | | 9 | 9 | 12 | 9 |
| KW 27 | 9 | 11 | 13 | 15 | 14 | 7 | 6 |
| KW 28 | 4 | 11 | 20 | 13 | 7 | 7 | 4 |
| KW 29 | 8 | 15 | 52 | 49 | 57 | 15 | 6 |
| KW 30 | 9 | 7 | 16 | 25 | 20 | 11 | |

| August | Montag | Dienstag | Mittwoch | Donnerstag | Freitag | Samstag | Sonntag |
|---|---|---|---|---|---|---|---|
| KW 30 | | | | | | | 7 |
| KW 31 | 13 | 15 | 15 | 21 | 19 | 13 | 8 |
| KW 32 | 14 | 14 | 14 | 15 | 17 | 14 | 8 |
| KW 33 | 11 | 19 | 26 | 30 | 33 | 19 | 3 |
| KW 34 | 16 | 22 | 73 | 74 | 2.440 | 2.435 | 6 |
| KW 35 | 6 | 9 | | | | | |

| September | Montag | Dienstag | Mittwoch | Donnerstag | Freitag | Samstag | Sonntag |
|---|---|---|---|---|---|---|---|
| KW 35 | | | 14 | 17 | 16 | 15 | 9 |
| KW 36 | 5 | 11 | 15 | 17 | 20 | 17 | 10 |
| KW 37 | 121 | 21 | 189 | 186 | 172 | 6 | 6 |
| KW 38 | 14 | 23 | 19 | 28 | 43 | 27 | 9 |
| KW 39 | 12 | 18 | 23 | 26 | | | |

| Legende | < 20 | ≥ 20 | ≥ 50 | ≥ 100 | ≥ 1.000 | ≥ 2.000 |
|---|---|---|---|---|---|---|

Im direkten Vergleich mit der Gesamtsituation im Bereich der Verkehrsdatenabfrage (vgl. oben Tabelle 9) ergeben sich bereits auf den ersten Blick deutlich erkennbare Unterschiede. Anders als bei den Maßnahmen nach § 33b BbgPolG werden hier lediglich in dem ersten Jahr einige Positionen sichtbar, an denen über mehrere aufeinanderfolgende Tage überhaupt kein Einsatz stattgefunden hat. Gut erkennbar wird auch, wie dann insbesondere in den letzten Monaten des Erhebungszeitraumes (drittes Quartal 2010) die Überwachungsintensität zugenommen hat. Hier gab es praktisch keine völlig überwachungsfreien Tage mehr. Täglich waren mindestens ein Dutzend, oft auch deutlich mehr Kennzeichen im aktiven Fahndungsbestand. Im vierten Quartal, das nicht mehr in den Evaluationszeitraum fällt, hat sich die Anzahl der Maßnahmen im Übrigen noch weiter erhöht (vgl. oben Tabelle 10). Durch die zunehmende Anzahl von Fahrzeugen, nach denen aktiv gefahndet wird, nimmt die Eingriffsbreite also insgesamt zu. Dies gilt auch dann, wenn man die Ausnahmeeinsätze aus den Bereichen Fußball und Rockeraktivitäten mit ihrer jeweils untypisch hohen Anzahl an Fahndungskennzeichen außer Betracht lässt.

Gleichwohl dürfte die Überwachungs-Gesamtlast in Brandenburg in Anbetracht des Verkehrsaufkommens insgesamt noch deutlich unterhalb dessen liegen, was das BVerfG auf der Grundlage der Kriterien, die es in seinem Grundsatzurteil zur automatischen Kennzeichenerfassung vom 11.3.2008 aufgestellt hat, als problematisch einordnen würde. Denn bei dem Schwergewicht der Fahndungen, die sich, wie aufgezeigt, jeweils auf ein einziges individuel-

les Kennzeichen konzentrieren, das für maximal einen Tag aktiv geschaltet wird, handelt es sich genau um diejenige Konstellation, die wegen des eigenen deliktischen Vorverhaltens der Betroffenen in der Bewertung des BVerfG am unteren Limit der Eingriffsintensität einzuordnen ist[310]. Eine flächendeckende Überwachungssituation ist darüber hinaus auch im Hinblick auf die begrenzte Anzahl existierender und tatsächlich eingesetzter Systeme nicht zu erkennen. Noch weniger kann von einer Totalüberwachung die Rede sein, die Kritiker dieser Technik grundsätzlich befürchten.

Die Praxis in Brandenburg dürfte auch bei einem weiteren moderaten Zuwachs der Fahndungsfälle noch als unbedenklich einzustufen sein. In Anbetracht der Unwägbarkeiten in der weiteren Entwicklung des Fallaufkommens, etwa bei den Kfz-Diebstählen, kann die Überwachungsdichte in der Zukunft jedenfalls durch die Entscheidung über einen möglichen weiteren Ausbau der Systeme – oder den Verzicht darauf – gesteuert werden.

---

310 BVerfG v. 11.3.2008, Abs. 78.

# Teil F: Abschließende Bewertung und Empfehlungen

Die Vielzahl der in diesem Gutachten präsentierten Ergebnisse kann an dieser Stelle nicht noch einmal wiederholt werden. Vielmehr sollen abschließend einige allgemeine Schlussfolgerungen skizziert werden, gefolgt von konkreten rechtspolitischen Empfehlungen zu den evaluierten Maßnahmen.

## 1. Allgemeines

1.1 Insgesamt ergibt sich aus den Ergebnissen, dass die Polizei in Brandenburg in verantwortungsvollem Umfang Gebrauch von den Ermächtigungen macht. Das belegen die insgesamt moderaten Anwendungszahlen zu allen drei evaluierten Maßnahmen.

1.2 Die zurückhaltende oder – wie im Fall des IMSI-Catchers – gar nur vereinzelte Anwendung einer Maßnahme indiziert nicht notwendigerweise ihre Überflüssigkeit. Spezielle Maßnahmen und ihre Rechtsgrundlagen können gerade für extreme Einzelsituationen konzipiert sein. Ein vergleichbares Beispiel hierfür ist die – mangels praktischer Anwendungsfälle – nicht in den Evaluationsauftrag einbezogene Maßnahme gem. § 33b Abs. 3 Nr. 3 BbgPolG (Unterdrücken von Telekommunikationsverbindungen). Hierbei handelt es sich um eine Ermächtigung für extreme Ausnahmesituationen. Ihre Existenz kann bei Eintritt einer entsprechenden Situation im Wortsinne Leben retten. Dasselbe gilt für den IMSI-Catcher, wenn man etwa an dessen Anwendungspotenzial zur Lokalisierung von Endgeräten (und ihres Trägers) beispielsweise im Fall einer Geiselnahme denkt.

1.3 Vorbildlich erscheint das Dokumentationssystem der Brandenburgischen Polizei. Zu allen Fällen waren zumindest Grundinformationen verfügbar. Wo zu bestimmten Fällen Akten geführt wurden, waren alle wesentlichen Informationen zu finden.

1.4 Rechtliche oder praktische Probleme bei der Durchführung der Maßnahmen waren nicht erkennbar. Die Anwendungspraxis achtet streng auf die Einhaltung der gesetzlichen Voraussetzungen.

1.5 Konkrete Empfehlungen beziehen sich daher ausschließlich auf die rechtliche Ebene. Sowohl bei der Verkehrsdatenabfrage als auch bei der anlassbezogenen automatischen Kennzeichenfahndung ergibt sich unter verfassungsrechtlicher Perspektive punktueller Anpassungsbedarf.

## 2. Verkehrsdatenabfrage (§ 33b Abs. 6 S. 2 BbgPolG)

2.1 Dies betrifft zunächst die fehlende gesetzliche Zweckbestimmung der Verkehrsdatenabfrage. Hierfür ergeben sich aus dem Urteil des BVerfG vom 2.3.2010 zur Vorratsdatenspeicherung klare Vorgaben. Danach ist ein präventiver Zugriff nur zulässig zur Abwehr von Gefahren für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des

Bundes oder des Landes oder zur Abwehr einer gemeinen Gefahr. Eine entsprechende Änderung erscheint zwingend.

2.2 Ergänzend könnte diskutiert werden, ob der in 2.1 umschriebene eng begrenzte Anwendungsbereich unter Wahrung der vom BVerfG aufgestellten Verhältnismäßigkeitskriterien eventuell erweiterungsfähig wäre. Die Verhältnismäßigkeit könnte möglicherweise auch unter erweiterten Anwendungsbedingungen noch gewahrt bleiben, wenn im Gegenzug die Eingriffsbreite der Maßnahme reduziert würde, etwa durch eine Limitierung der Zugriffsmöglichkeit auf einzelne Datenarten, insbesondere die für die Lokalisierung im Bereich der Gefahrenabwehr so wichtigen Standortdaten. Weitere Begrenzungen in Form einer Konzentration auf Echtzeitdaten oder Daten aus einem bestimmten, zeitlich vordefinierten Zeitraum erscheinen ebenfalls denkbar. Ob ein genereller Verzicht auf einzelne Datenarten oder ältere Daten polizeitaktisch sinnvoll und vertretbar wäre, kann auf der Basis der hier verfügbaren Daten allerdings nicht beurteilt werden. Dass im Einzelfall, in dem aktuelle Geodaten nicht verfügbar sind, auch andere Verkehrsdaten (beispielsweise Ort oder Identität eines häufigen Anrufers) Anhaltspunkte für einen möglichen Aufenthaltsort zu geben vermögen, bleibt denkbar, auch wenn dies im Evaluationszeitraum in keinem Fall von Bedeutung war. Im Gegenzug wäre ebenfalls zu klären, ob weitere als die gegenwärtig geregelten Anwendungsfälle überhaupt praxisrelevant wären.

2.3 Einer Neuregelung bedarf zwingend auch die Frage des Richtervorbehaltes. Dabei kann in der Substanz auf die Regelungen des Erlasses vom 14.7.2010 zurückgegriffen werden. Insbesondere die dortigen Bestimmungen zu den vier Fällen von Gefahr im Verzug, zu der Definition des Verzugs sowie zu den Zuständigkeiten erscheinen sachgerecht.

2.4 In Anbetracht des Umfanges der erforderlichen Regelungen zur Zweckbestimmung und zum Richtervorbehalt empfiehlt sich unseres Erachtens die Überführung des bisherigen Satzes 2 in einen eigenen Absatz.

2.5 Eine redaktionelle Änderung ist darüber hinaus in § 33b Abs. 6 S. 3 BbgPolG zu empfehlen: Das dort in Bezug genommene JVEG heißt korrekt „Justizvergütungs- und Entschädigungsgesetz".

2.6 Im Übrigen wird die Verfügbarkeit von Verkehrsdaten von der Ausgestaltung der entsprechenden Regelungen des TKG abhängen, die im Rahmen der Neuregelung der Vorratsdatenspeicherung sicherlich eine Veränderung erfahren werden. Auf einen expliziten Verweis auf bestimmte Rechtsgrundlagen zur Datenspeicherung im TKG nach dem Vorbild des § 100g StPO sollte daher zumindest im gegenwärtigen Stadium verzichtet werden. Die weitere rechtliche Entwicklung ist, wie eingangs erläutert, noch nicht absehbar. Auch nach einer Neuregelung der Vorratsdatenspeicherung auf Bundesebene ist mit weiteren Änderungen, etwa in Folge einer Überarbeitung der EU-rechtlichen Vorgaben, zu rechnen. Im Übrigen ist das Telekommunikationsrecht durch seine Abhängigkeit von den technischen Entwicklungen generell änderungsanfällig.

2.7 Ein alternatives Instrument, das als funktionales Äquivalent zu der präventiven Verkehrsdatenabfrage eingesetzt werden könnte, steht auf der Basis des gegenwärtig im

BbgPolG vorgesehenen polizeilichen Maßnahmenkataloges nicht zur Verfügung. Die Maßnahme hat ein sehr spezifisches Einsatzpozenzial und ist auf die weiträumige und zugleich schnelle Suche nach akut gefährdeten Personen angelegt. Die Polizei ist für die Ermittlung des nicht bekannten Aufenthaltsortes solcher Personen auf die Unterstützung durch die technischen Daten der Telekommunikationsanbieter zwingend angewiesen. Nur diese Daten erlauben eine zeitnahe Lokaliserung der konkreten Zielperson oder zumindest eine an dem individuellen Bewegungsverhalten orientierte Eingrenzung ihres mutmaßlichen Aufenthaltsortes. Im Idealfall stehen diese sogar in Echtzeit oder zumindest für einen nur kurz zurückliegenden Zeitpunkt zur Verfügung. Die Polizei ist weder technisch noch rechtlich in der Lage, vergleichbare Informationen selbst zu erheben; schon gar nicht seit der Privatisierung des Telekommunikationssektors.

## 3. Anlassbezogene automatische Kennzeichenfahndung (§ 36a BbgPolG)

3.1 Zur Kennzeichenfahndung ist zunächst festzustellen, dass die in Brandenburg eingeführte Terminologie der anlassbezogenen automatischen Kennzeichenfahndung im Vergleich zu alternativen Bezeichnungen in anderen Bundesländern unbedingt vorzugswürdig erscheint.

3.2 Der in § 36a BbgPolG normierte Regelungszusammenhang zwischen weit gefasstem Verwendungszweck der erhobenen Daten einerseits bei gleichzeitig eng begrenzten Eingriffsvoraussetzungen andererseits erscheint als gut gelungener Ausgleich zur Wahrung der Verhältnismäßigkeit. Demensprechend hat die Regelung in dem Urteil des BVerfG vom 11.3.2008 zur Kennzeichenfahndung positive Erwähnung gefunden.

3.3 Zwingender Nachbesserungsbedarf wird ausschließlich im Hinblick auf den Spezialfall der manuellen Überprüfung möglicher Fehltreffer gesehen. Für diese Situation fordert das BVerfG eine unverzügliche Überprüfung und sofortige Löschung. § 36a Abs. 2 BbgPolG regelt diesen Fall nicht gesondert. Die Praxis entspricht nach den Ergebnissen der Evaluation zwar den Vorgaben des BVerfG. Die gesetzliche Grundlage sollte dem aber auch tatsächlich angeglichen werden.

3.4 Zur Diskussion gestellt werden soll abschließend noch einmal die aktuelle Behandlung der Totalentwendungsfälle. Sie sind derzeit nicht durch die Ermächtigung des § 36a Abs. 1 BbgPolG umfasst, sondern werden auf der Grundlage von § 100h Abs. 1 Nr. 2 StPO in die Kennzeichenfahndung übernommen. Damit fällt ausgerechnet die häufigste Anwendungsvariante der automatischen Kennzeichenfahndung aus dem Anwendungsbereich des § 36a BbgPolG heraus. Dies berücksichtigt unseres Erachtens auch den Doppelcharakter des Autodiebstahls nur unzureichend. Anders als bei vielen anderen Straftaten dient die Ermittlung gestohlener Fahrzeuge nicht nur der Beweissicherung im Strafverfahren, sondern zugleich auch der Beendigung der Eigentumsstörung durch Rückführung an den Eigentümer. Diese originär präventive Komponente dieser Fallkonstellation wird in der gegenwärtigen Rechtslage nicht adäquat reflektiert.

3.5 Möglicherweise könnte mit der Aufnahme des Kfz-Diebstahls in den Anwendungsbereich § 36a BbgPolG auch eine Effizienzsteigerung erreicht werden. Denn mit der Loslösung aus dem Normengefüge der StPO könnte auch die aktuelle Praxis, Eilfahndungen auf eine Dauer von 23:59 h zu begrenzen, überdacht werden. Für die insgesamt geringe Trefferquote sind namentlich zwei Ursachen wahrscheinlich. Einerseits dürften viele Fahrzeuge bereits jenseits der Landesgrenzen verbracht worden sein, wenn der Diebstahl bemerkt wird. Die Aufschaltung des Kennzeichens kommt dann schlicht zu spät. Andererseits kann auch die kurze Fahndungsdauer eine Ursache setzen. Im Hinblick auf die Zielgenauigkeit, die faktisch ausschließt, dass Nichtbetroffene von der Maßnahme tangiert werden, erscheint zumindest eine moderate, ggf. testweise Verlängerung, beispielsweise auf 48 oder 72 Stunden, vorstellbar. Um zu vermeiden, dass sich bei einer allzu langen Fahndungsdauer ein sehr umfangreicher Datenbestand ansammelt, sollte dies freilich auf einige Tage begrenzt werden. Andernfalls wäre es auch keine anlassbezogene Maßnahme mehr.

3.6 Die Frage nach möglichen funktionalen Äquivalenten ist hier etwas differenzierter zu bewerten, im Ergebnis aber in dem gleichen Tenor zu beantworten wie im Falle der Verkehrsdatenabfrage. Bei der Kennzeichenfahndung wäre für einzelne Einsatzvarianten, beispielsweise mobile Kontrollen im Vorfeld von Veranstaltungen oder längerfristige Observationen, ein partieller Ersatz durch herkömmliche Maßnahmen zwar denkbar. Dies würde freilich den Einsatz erheblicher Personalressourcen bei dem Wach- und Wechseldienst erfordern, der im Hinblick auf die mittelfristige Haushaltsentwicklung schwer darstellbar erscheint. Die Lesekapazität der in Brandenburg eingesetzten Systeme übertrifft diejenige des menschlichen Auges um ein Vielfaches. Die automatische Kennzeichenfahndung erscheint in dieser Hinsicht ungleich effektiver. Im Hinblick auf die Fahndung nach gestohlenen Kraftfahrzeugen ist sie zudem effizienter. Dies gilt insbesondere dann, wenn die stationären Geräte zum Einsatz kommen, die gleichzeitig, ohne zeitliche Verzögerung und zu jeder Tages- und Nachtzeit aktiviert werden können. Hier handelt es sich wiederum um eine weiträumig angelegte Suche ohne konkrete Anhaltspunkte zu einem bestimmten Aufenthaltsort, ähnlich der Konstellation bei der Lokalisierung durch Telekommunikations-Geodaten. Eine einzelne Kontrollstelle hätte unter allen hier genannten Aspekten eine sehr viel geringere Trefferwahrscheinlichkeit, selbst wenn sie ebenso lange eingerichtet bliebe wie die gegenwärtige Dauer einer einzelnen Kennnzeichenfahndung (vgl. Pkt. 3.5. – eine Prämisse, die überdies wenig realitsätsnah erschiene). Die Verfügbarkeit der automatischen Lesesysteme entlastet die Polizei zudem von einem Teil ihrer straßenverkehrs- bzw. Kfz-bezogenen Aufgaben und erlaubt so eine andere Prioritätensetzung bei dem Einsatz der Beamtinnen und Beamten.

## 4. Formulierungsvorschläge

Unter Berücksichtigung der vorstehnden Empfehlungen werden abschließend zwei Formulierungsvorschläge für die anstehende Novellierung der §§ 33b Abs. 6 und 36a BbgPolG präsentiert. Im Hinblick auf § 33b Abs. 3 BbgPolG wird kein Änderungsbedarf gesehen.

Inhaltliche und redaktionelle Änderungen sind besonders gekennzeichnet.

*§ 33b BbgPolG-Vorschlag_MPI*

Datenerhebung durch Eingriffe in die Telekommunikation

(1) Die Polizei kann unter den Voraussetzungen des § 33a Abs. 1 personenbezogene Daten durch den verdeckten Einsatz technischer Mittel zur Überwachung und Aufzeichnung der Telekommunikation erheben.

(2) [1]Die Befugnis nach Absatz 1 berechtigt zur Datenerhebung nur über die Person des für die Gefahr Verantwortlichen oder eines Notstandspflichtigen und zu Eingriffen in die Telekommunikation dieser Personen. [2]Zum Zwecke der vorbeugenden Bekämpfung von Straftaten berechtigt die Befugnis nach Absatz 1 zur Datenerhebung nur über die Person des potenziellen Straftäters oder seiner Kontakt- oder Begleitpersonen (§ 33a Abs. 2 Satz 3 bis 5) und zu Eingriffen in die Telekommunikation dieser Personen. [3]Wird erkennbar, dass in den Kernbereich privater Lebensgestaltung oder in ein durch ein Berufsgeheimnis nach §§ 53, 53a der Strafprozessordnung geschütztes Vertrauensverhältnis eingegriffen wird, ist die Datenerhebung zu unterbrechen, es sei denn, sie richtet sich gegen den Berufsgeheimnisträger selbst.

(3) Die Polizei kann unter den Voraussetzungen der Absätze 1 und 2 auch technische Mittel einsetzen, um

1. spezifische Kennungen, insbesondere Geräte- und Kartennummer von Mobilfunkendgeräten, zu ermitteln, wenn dies für die Durchführung einer Maßnahme nach Absatz 1 unerlässlich ist,
2. den Standort eines Mobilfunkendgerätes zu ermitteln oder
3. Telekommunikationsverbindungen zu unterbrechen oder zu verhindern.

(4) [1]Bei Maßnahmen nach Absatz 1 und 3 dürfen personenbezogene Daten Dritter nur erhoben und Telekommunikationsverbindungen Dritter nur unterbrochen oder verhindert werden, wenn dies zu ihrer Durchführung unvermeidbar ist und zum Zwecke der Maßnahme nicht außer Verhältnis steht. [2]Nach Beendigung der Maßnahme sind dabei erhobene Daten unverzüglich zu löschen.

(5) [1]Die Maßnahme darf nur durch den Richter, bei Gefahr im Verzug auch durch den Behördenleiter angeordnet werden; in diesem Fall ist unverzüglich eine richterliche Bestätigung einzuholen. [2]Zuständig ist das Amtsgericht, in dessen Bezirk die beantragende Polizeibehörde ihren Sitz hat. [3]Für das Verfahren gelten die Vorschriften des [*Gesetzes über die Angelegenheiten der freiwilligen Gerichtsbarkeit*] entsprechend. [4]In der schriftlichen Anordnung sind anzugeben

1. soweit bekannt, der Name und die Anschrift des Adressaten, gegen den sich die Maßnahme richtet,
2. eine Kennung des Telekommunikationsanschlusses oder Endgerätes,
3. die Art der Maßnahme sowie

4. die tragenden Erkenntnisse für das Vorliegen der Gefahr nach Absatz 1 und die Begründung der Verhältnismäßigkeit der Maßnahme.

[5]Die Anordnung ist auf den nachfolgend genannten Zeitraum zu befristen:

1. im Falle des Absatzes 3 Nr. 2 höchstens zwei Wochen,
2. im Falle des Absatzes 3 Nr. 3 höchstens drei Tage und
3. in allen anderen Fällen höchstens einen Monat.

[6]Eine Verlängerung um jeweils den gleichen Zeitraum ist zulässig, sofern die Anordnungsvoraussetzungen fortbestehen. [7]Anderenfalls ist die Maßnahme unverzüglich zu beenden und das anordnende Gericht darüber zu benachrichtigen.

**(6) [1]Die Polizei kann zur Abwehr einer Gefahr für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder des Landes oder zur Abwehr einer gemeinen Gefahr Diensteanbieter verpflichten, unverzüglich Auskunft über vorhandene Verkehrsdaten der in Absatz 2 genannten Personen sowie über die für die Ermittlung des Standortes eines Mobilfunkendgerätes dieser Personen erforderlichen spezifischen Kennungen, insbesondere die Geräte- und Kartennummer sowie die Zellinformationen, zu erteilen. [2]Eine Auskunftsanordnung über künftig anfallende Verkehrs- oder Standortdaten ist nach Maßgabe des Absatzes 5 Satz 5 Nr. 1 zu befristen; eine Verlängerung um jeweils den gleichen Zeitraum ist zulässig, sofern die Anordnungsvoraussetzungen fortbestehen. [3]Die Maßnahme darf nur durch den Richter, bei Gefahr im Verzug auch durch den Behördenleiter oder seinen Vertreter im Amt, angeordnet werden; in diesem Fall ist unverzüglich eine richterliche Bestätigung einzuholen; Gefahr im Verzug ist insbesondere anzunehmen, wenn für die**

1. **Beseitigung einer Suizidgefahr,**
2. **Suche nach gefährdeten Vermissten,**
3. **Suche nach minderjährigen Vermissten oder**
4. **die Befreiung aus einer hilflosen Lage**

**aufgrund einer Prüfung im Einzelfall die Zeit fehlt, vor dem Auskunftsersuchen einen Richter zu erreichen. [4]Im Übrigen gelten die Bestimmungen des Absatzes 5 zur Zuständigkeit und zum Verfahren entsprechend.**

(7) [1]Eine Anordnung nach den **Absätzen 5 und 6** verpflichtet jeden, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt (Diensteanbieter), nach Maßgabe der Regelungen des Telekommunikationsgesetzes und der darauf beruhenden Rechtsverordnungen zur technischen und organisatorischen Umsetzung von Überwachungsmaßnahmen in der jeweils geltenden Fassung der Polizei die Überwachung und Aufzeichnung zu ermöglichen. [2]Die Entschädigung richtet sich nach § 23 des **Justizvergütungs- und Entschädigungsgesetzes**, soweit nicht eine Entschädigung aufgrund des Telekommunikationsgesetzes zu gewähren ist.

**(8)** Die Unterrichtung des Betroffenen richtet sich nach § 29 Abs. 7 und 8 sowie § 33a Abs. 6.

**(9)** [1]Die aufgrund einer Maßnahme nach Absatz 1, 3 und 6 Satz 2 erlangten personenbezogenen Daten sind besonders zu kennzeichnen. [2]Sie dürfen für andere Zwecke verwendet werden, wenn dies zur Abwehr einer in Absatz 1 genannten Gefahr für die öffentliche Sicherheit oder für die Verfolgung von Straftaten nach § 100a Satz 1 der Strafprozessordnung erforderlich ist. [3]Eine solche Änderung der Zweckrichtung ist festzustellen und zu dokumentieren.

**(10)** [1]Daten, bei denen sich nach der Auswertung herausstellt, dass die Voraussetzungen für ihre Erhebung nicht vorlagen, dürfen nicht verwendet werden und sind unverzüglich zu löschen, es sei denn, ihre Verwendung ist zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erforderlich. [2]In diesen Fällen ist eine richterliche Entscheidung über die Zulässigkeit der Verwendung unverzüglich einzuholen; Absatz 5 gilt entsprechend. [3]Im Übrigen sind die aufgrund von Maßnahmen nach Absatz 1, 3 und 6 Satz 2 erlangten personenbezogenen Daten unverzüglich zu sperren, wenn sie nicht mehr erforderlich sind. [4]Sie dürfen ausschließlich für eine gerichtliche Überprüfung verwendet werden und sind unverzüglich zu löschen, wenn sie hierfür nicht benötigt werden, spätestens jedoch zwei Wochen nach Unterrichtung der Betroffenen. [5]Auf diese Frist ist in der Unterrichtung hinzuweisen. [6]Die Löschung von Daten nach Satz 1 und 4 und nach Absatz 4 Satz 2 ist zu dokumentieren.

**(11)** [1]Das für Inneres zuständige Mitglied der Landesregierung erstattet dem Ausschuss für Inneres des Landtages jährlich einen Bericht über jede Maßnahme. [2]§ 33a Abs. 9 gilt entsprechend.

*§ 36a BbgPolG-Vorschlag_MPI*

Anlassbezogene automatische Kennzeichenfahndung

(1) Die Polizei kann die Kennzeichen von Fahrzeugen ohne Wissen der Person durch den Einsatz technischer Mittel automatisiert erheben, wenn

1. dies zur Abwehr einer gegenwärtigen Gefahr für Leib oder Leben einer Person erforderlich ist,
2. dies zur Abwehr einer gegenwärtigen Gefahr erforderlich ist und die Voraussetzungen für eine Identitätsfeststellung nach § 12 Abs. 1 Nr. 2 bis 4 vorliegen,
3. **das Kraftfahrzeug innerhalb der letzten [vierundzwanzig oder achtundvierzig oder zweiundsiebzig] Stunden als entwendet gemeldet wurde, oder**
4. eine Person oder ein Fahrzeug nach § 36 Abs. 1 und 1a polizeilich ausgeschrieben wurde und Tatsachen die Annahme rechtfertigen, dass die für die Ausschreibung relevante Begehung von Straftaten unmittelbar bevorsteht.

(2) [1]Die erhobenen Daten können mit zur Abwehr der Gefahr nach Absatz 1 gespeicherten polizeilichen Daten automatisch abgeglichen werden. [2]**Im Trefferfall ist unverzüglich die Datenübereinstimmung zu überprüfen.** [3]Bei Datenübereinstimmung können die Daten polizeilich verarbeitet und im Falle des Absatzes 1 Nr. 4 zusammen mit den gewonnenen Erkenntnissen an die ausschreibende Stelle übermittelt werden. [4]Andernfalls sind sie **sofort** zu löschen.

(3) Das für Inneres zuständige Mitglied der Landesregierung erstattet dem Ausschuss für Inneres des Landtages jährlich einen Bericht über jede Maßnahme, der Angaben enthält über deren Anlass, Ort und Dauer.

# Teil G: Anhänge

## 1. Aktuelle Gesetzestexte

*§ 33b BbgPolG*

Datenerhebung durch Eingriffe in die Telekommunikation

(1) Die Polizei kann unter den Voraussetzungen des § 33a Abs. 1 personenbezogene Daten durch den verdeckten Einsatz technischer Mittel zur Überwachung und Aufzeichnung der Telekommunikation erheben.

(2) [1]Die Befugnis nach Absatz 1 berechtigt zur Datenerhebung nur über die Person des für die Gefahr Verantwortlichen oder eines Notstandspflichtigen und zu Eingriffen in die Telekommunikation dieser Personen. [2]Zum Zwecke der vorbeugenden Bekämpfung von Straftaten berechtigt die Befugnis nach Absatz 1 zur Datenerhebung nur über die Person des potenziellen Straftäters oder seiner Kontakt- oder Begleitpersonen (§ 33a Abs. 2 Satz 3 bis 5) und zu Eingriffen in die Telekommunikation dieser Personen. [3]Wird erkennbar, dass in den Kernbereich privater Lebensgestaltung oder in ein durch ein Berufsgeheimnis nach §§ 53, 53a der Strafprozessordnung geschütztes Vertrauensverhältnis eingegriffen wird, ist die Datenerhebung zu unterbrechen, es sei denn, sie richtet sich gegen den Berufsgeheimnisträger selbst.

(3) Die Polizei kann unter den Voraussetzungen der Absätze 1 und 2 auch technische Mittel einsetzen, um

4. spezifische Kennungen, insbesondere Geräte- und Kartennummer von Mobilfunkendgeräten, zu ermitteln, wenn dies für die Durchführung einer Maßnahme nach Absatz 1 unerlässlich ist,
5. den Standort eines Mobilfunkendgerätes zu ermitteln oder
6. Telekommunikationsverbindungen zu unterbrechen oder zu verhindern.

(4) [1]Bei Maßnahmen nach Absatz 1 und 3 dürfen personenbezogene Daten Dritter nur erhoben und Telekommunikationsverbindungen Dritter nur unterbrochen oder verhindert werden, wenn dies zu ihrer Durchführung unvermeidbar ist und zum Zwecke der Maßnahme nicht außer Verhältnis steht. [2]Nach Beendigung der Maßnahme sind dabei erhobene Daten unverzüglich zu löschen.

(5) [1]Die Maßnahme darf nur durch den Richter, bei Gefahr im Verzug auch durch den Behördenleiter angeordnet werden; in diesem Fall ist unverzüglich eine richterliche Bestätigung einzuholen. [2]Zuständig ist das Amtsgericht, in dessen Bezirk die beantragende Polizeibehörde ihren Sitz hat. [3]Für das Verfahren gelten die Vorschriften des Gesetzes über die Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. [4]In der schriftlichen Anordnung sind anzugeben

5. soweit bekannt, der Name und die Anschrift des Adressaten, gegen den sich die Maßnahme richtet,
6. eine Kennung des Telekommunikationsanschlusses oder Endgerätes,
7. die Art der Maßnahme sowie
8. die tragenden Erkenntnisse für das Vorliegen der Gefahr nach Absatz 1 und die Begründung der Verhältnismäßigkeit der Maßnahme.

[5] Die Anordnung ist auf den nachfolgend genannten Zeitraum zu befristen:

4. im Falle des Absatzes 3 Nr. 2 höchstens zwei Wochen,
5. im Falle des Absatzes 3 Nr. 3 höchstens drei Tage und
6. in allen anderen Fällen höchstens einen Monat.

[6] Eine Verlängerung um jeweils den gleichen Zeitraum ist zulässig, sofern die Anordnungsvoraussetzungen fortbestehen. [7] Anderenfalls ist die Maßnahme unverzüglich zu beenden und das anordnende Gericht darüber zu benachrichtigen.

(6) [1] Eine Anordnung nach Absatz 5 verpflichtet jeden, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt (Diensteanbieter), nach Maßgabe der Regelungen des Telekommunikationsgesetzes und der darauf beruhenden Rechtsverordnungen zur technischen und organisatorischen Umsetzung von Überwachungsmaßnahmen in der jeweils geltenden Fassung der Polizei die Überwachung und Aufzeichnung zu ermöglichen. [2] Die Polizei kann Diensteanbieter unter den Voraussetzungen der Absätze 1 und 2 verpflichten, unverzüglich Auskunft über vorhandene und künftige Verkehrsdaten der dort genannten Personen sowie über die für die Ermittlung des Standortes eines Mobilfunkendgerätes dieser Personen erforderlichen spezifischen Kennungen, insbesondere die Geräte- und Kartennummer sowie die Zellinformationen, zu erteilen. [3] Die Entschädigung richtet sich nach § 23 des Justizvergütungsgesetzes, soweit nicht eine Entschädigung aufgrund des Telekommunikationsgesetzes zu gewähren ist.

(7) Die Unterrichtung des Betroffenen richtet sich nach § 29 Abs. 7 und 8 sowie § 33a Abs. 6.

(8) [1] Die aufgrund einer Maßnahme nach Absatz 1, 3 und 6 Satz 2 erlangten personenbezogenen Daten sind besonders zu kennzeichnen. [2] Sie dürfen für andere Zwecke verwendet werden, wenn dies zur Abwehr einer in Absatz 1 genannten Gefahr für die öffentliche Sicherheit oder für die Verfolgung von Straftaten nach § 100a Satz 1 der Strafprozessordnung erforderlich ist. [3] Eine solche Änderung der Zweckrichtung ist festzustellen und zu dokumentieren.

(9) [1] Daten, bei denen sich nach der Auswertung herausstellt, dass die Voraussetzungen für ihre Erhebung nicht vorlagen, dürfen nicht verwendet werden und sind unverzüglich zu löschen, es sei denn, ihre Verwendung ist zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erforderlich. [2] In diesen Fällen ist eine richterliche Entscheidung über die Zulässigkeit der Verwendung unverzüglich einzuholen; Absatz 5 gilt entspre-

chend. [3]Im Übrigen sind die aufgrund von Maßnahmen nach Absatz 1, 3 und 6 Satz 2 erlangten personenbezogenen Daten unverzüglich zu sperren, wenn sie nicht mehr erforderlich sind. [4]Sie dürfen ausschließlich für eine gerichtliche Überprüfung verwendet werden und sind unverzüglich zu löschen, wenn sie hierfür nicht benötigt werden, spätestens jedoch zwei Wochen nach Unterrichtung der Betroffenen. [5]Auf diese Frist ist in der Unterrichtung hinzuweisen. [6]Die Löschung von Daten nach Satz 1 und 4 und nach Absatz 4 Satz 2 ist zu dokumentieren.

(10) [1]Das für Inneres zuständige Mitglied der Landesregierung erstattet dem Ausschuss für Inneres des Landtages jährlich einen Bericht über jede Maßnahme. [2]§ 33a Abs. 9 gilt entsprechend.

*§ 36a BbgPolG*

Anlassbezogene automatische Kennzeichenfahndung

(1) Die Polizei kann die Kennzeichen von Fahrzeugen ohne Wissen der Person durch den Einsatz technischer Mittel automatisiert erheben, wenn

5. dies zur Abwehr einer gegenwärtigen Gefahr für Leib oder Leben einer Person erforderlich ist,
6. dies zur Abwehr einer gegenwärtigen Gefahr erforderlich ist und die Voraussetzungen für eine Identitätsfeststellung nach § 12 Abs. 1 Nr. 2 bis 4 vorliegen oder
7. eine Person oder ein Fahrzeug nach § 36 Abs. 1 und 1a polizeilich ausgeschrieben wurde und Tatsachen die Annahme rechtfertigen, dass die für die Ausschreibung relevante Begehung von Straftaten unmittelbar bevorsteht.

(2) [1]Die erhobenen Daten können mit zur Abwehr der Gefahr nach Absatz 1 gespeicherten polizeilichen Daten automatisch abgeglichen werden. [2]Bei Datenübereinstimmung können die Daten polizeilich verarbeitet und im Falle des Absatzes 1 Nr. 3 zusammen mit den gewonnenen Erkenntnissen an die ausschreibende Stelle übermittelt werden. [3]Andernfalls sind sie unverzüglich zu löschen.

(3) Das für Inneres zuständige Mitglied der Landesregierung erstattet dem Ausschuss für Inneres des Landtages jährlich einen Bericht über jede Maßnahme, der Angaben enthält über deren Anlass, Ort und Dauer.

## 2. Protokoll der Expertengespräche

*Hinweis: Im Rahmen des Moduls „Expertengespräche 2" wurden Verständnisfragen zu einzelnen Sachverhalten und Einsätzen geklärt. Ein Abdruck des Protokolls ohne die entsprechenden Fallakten wäre wenig aufschlussreich, die Veröffentlichung der jeweiligen Akteninhalte ist aus datenschutzrechtlichen Gründen jedoch nicht möglich. Aus diesem Grund wird auf die Wiedergabe des Protokolls zum Modul „Expertengespräche 2" verzichtet und im Folgenden lediglich das Protokoll des Moduls „Expertengespräche 1" abgedruckt.*

Cottbus und Potsdam, 29. und 30. Oktober 2009

Expertengespräche beim

- Polizeipräsidium Frankfurt (Oder), Schutzbereich Cottbus / Spree-Neiße (Kennzeichenfahndung)
- LKA Brandenburg, Außenstelle Potsdam (IMSI-Catcher)
- Polizeipräsidium Potsdam (IMSI-Catcher, Verkehrsdatenabfrage)

*Hinweis: Im Folgenden handelt es sich um Ergebnisniederschriften. Auf eine Zurechenbarkeit der Antworten zu einzelnen Interviewpartnern wurde bewusst verzichtet, wie diese aus Datenschutzgründen auch namentlich unidentifizierbar bleiben sollen.*

### 1. Allgemeine Fragen

**1.1** Durch Schengen sind die Grenzkontrollen an den Binnengrenzen der Mitgliedsstaaten weggefallen. Sicherheit muss nun auf andere Weise gewährleistet werden. In einem 30 km breiten Streifen entlang der Bundesgrenzen dürfen daher mobile Grenzkontrollen durchgeführt werden. Kommt die automatische Kennzeichenfahndung im Rahmen dieser mobilen Grenzkontrollen zum Einsatz?

*Ja, die automatische Kennzeichenfahndung kann auch im Rahmen solcher mobilen Grenzkontrollen durchgeführt werden. Ihre Zulässigkeit richtet sich dabei nach dem Polizeigesetz des jeweiligen Landes. Da der Zoll und die Bundespolizei keine eigenen Geräte zur Durchführung der automatischen Kennzeichenfahndung besitzen, können sie die Polizei des Landes Brandenburg um Amtshilfe bitten. Der Zoll hat eine entsprechende Anfrage bereits mehrfach gestellt, eine Anfrage der Bundespolizei ist bei der Polizei des Landes Brandenburg bislang noch nicht eingegangen.*

**1.2** Nach § 99 SDÜ können Personen oder Fahrzeuge auch dann zur Fahndung ausgeschrieben werden, wenn dies zur Abwehr von Gefahren für die öffentliche Sicherheit erforderlich ist. Auf welche Ermächtigungsgrundlage stützt sich eine Fahndung, die infolge einer solchen Ausschreibung durchgeführt wird: auf nationales Recht oder auf das SDÜ selbst?

*Das SDÜ hält keine Ermächtigungsgrundlage für die automatische Kennzeichenfahndung bereit. Die Durchführung richtet sich immer nach § 36a BbgPolG.*

**1.3** Wie wird ein Richtervorbehalt praktisch umgesetzt?

**a)** Gibt es eine zentrale Kontaktstelle, die alle Anträge routinemäßig vorbereitet und stellt?

*Es gibt keine zentrale Kontaktstelle. Die Polizei (z.B. die Leitstelle) stellt einen Antrag bei dem jeweils zuständigen Amtsgericht.*

**b)** Wie lange dauert es i.d.R. bis zum Beschluss?

*Tagsüber kann relativ schnell mit einer Antwort des zuständigen Richters gerechnet werden; der Beschluss ergeht häufig schon binnen einer Stunde, auf jeden Fall aber noch am selben Tag. Nachts kann es etwas länger dauern. Es gibt jedoch einen Eildienst-Richter, der rund um die Uhr erreichbar ist.*

*Soll eine Maßnahme, die einem Richtervorbehalt unterliegt, zur Prävention von Straftaten durchgeführt werden, ist eine besonders umfassende Begründung erforderlich. Erst wenn dem Richter eine umfassende Begründung vorliegt, kann in diesen Fällen mit einem richterlichen Beschluss gerechnet werden. Daher hängt es unter anderem von der Genauigkeit und dem Umfang der Vorarbeiten ab, wie lange es dauert, bis eine richterliche Anordnung ergeht.*

*Die Zusammenarbeit mit den zuständigen Richtern funktioniert in der Regel sehr gut. Häufig wird die Anfrage zunächst telefonisch gestellt und eine mündliche Zusage erteilt. Der schriftliche Antrag wird dann unverzüglich nachgereicht.*

*Selbst bei der Verkehrsdatenabfrage, die in Brandenburg keinem Richtervorbehalt unterliegt, wird regelmäßig ein richterlicher Beschluss eingeholt, bevor die Maßnahme durchgeführt wird. Der Richtervorbehalt stellt also in der Praxis keine Erschwernis i.R.d. polizeilichen Tätigkeit dar.*

**2. Automatische Kennzeichenfahndung** (§ 36a BbgPolG)

**2.1** Worin liegt der Unterschied zwischen einer automatischen Kennzeichenfahndung, wie sie in § 36a BbgPolG vorgesehen ist, und einer automatischen Kennzeichenerfassung i.S.d. Strafprozessordnung (§§163f, 100h, 111,163e StPO)?

*Bei einer automatischen Kennzeichenfahndung wird gezielt nach einzelnen Fahrzeugen gesucht. Fährt eines der gesuchten Fahrzeuge an einer Kontrolleinrichtung vorbei, werden die Daten dieses Fahrzeuges – nur dieses Fahrzeuges – erfasst und gespeichert.*

*Im Rahmen einer Kennzeichenerfassung hingegen werden alle Fahrzeuge, die das Kontrollgerät passieren, erfasst und die dazugehörigen Kennzeichen gespeichert. Diese Maßnahme ist nur nach der StPO zulässig und steht dort unter einem Richtervorbehalt. Derzeit wird eine solche systematische, repressive Kennzeichenerfassung im Rahmen eines Verfahrens zur Bekämpfung der organisierten Kriminalität einen Monat lang durchgeführt. Das BbgPolG enthält keine Rechtsgrundlage für eine Kennzeichenerfassung. Zur Gefahrenabwehr ist also nur eine Kennzeichenfahndung zulässig.*

*Technisch wäre es möglich, beide Maßnahmen gleichzeitig durchzuführen. Beide Maßnahmen werden von demselben Einsatzteam durchgeführt.*

**2.2** Wie viele Geräte zur automatischen Kennzeichenfahndung gibt es in Brandenburg? Wie viele davon sind stationäre, wie viele mobile Geräte?

*In Brandenburg gibt es drei mobile und drei stationäre Geräte. Von den mobilen Geräten befinden sich zwei bei der Bereitschaftspolizei Cottbus und eines bei Spezialeinheiten des LKA. Die stationären Geräte wurden an taktisch günstigen Orten angebracht. Geplant ist, dass in Brandenburg insgesamt acht stationäre Anlagen eingesetzt werden. Die endgültige Entscheidung darüber liegt jedoch beim Innenministerium.*

**2.3** § 36a BbgPolG spricht davon, dass ein Abgleich mit „für die Aufgabe der Gefahrenabwehr gespeicherten Daten" zulässig ist. Welche Daten enthält die Suchdatei?

*Zunächst enthält die Datei das gesuchte Kennzeichen. Dieses wird von der Anwendungssoftware zusammengezogen, Leerzeichen und Fremdkörper werden also nicht erfasst. Wird z.B. nach dem Kennzeichen TE-ST 1234 gesucht, wird es von dem System zu TEST1234 umgewandelt. Des Weiteren wird in der Datei festgehalten, wann das Kennzeichen in die Liste aufgenommen wurde (Datum und Uhrzeit) und wie lange es in der Datei gespeichert bleiben soll. Es ist also möglich, die Fahndung nach einem bestimm-*

*ten Kennzeichen zeitlich zu begrenzen. Bei gestohlenen Kfz beträgt die Fahndungsdauer bspw. 24 Stunden. Ferner können Bemerkungen in die Datei eingespeist werden, die Aufschluss über den Grund der Fahndung geben, die gesuchte Person einer Verdächtigengruppe zuordnen oder den Rückgriff auf eine Polizeiakte ermöglichen. Allerdings haben nur wenige Personen Zugriff auf die Fahndungsdatei. Die Eingabe-, Einsichts- und Zugriffsrechte sind genau geregelt.*

**2.4** Wie viele Kennzeichen können maximal in das System eingegeben werden? Nach wie vielen Kennzeichen kann gleichzeitig gefahndet werden? Können auch ganze Fahndungslisten in die Datei geladen werden?

*Es können beliebig viele Kennzeichen in das System eingegeben werden. Auch ganze Fahndungslisten können in das System eingespeist werden. Sowohl auf Bundes- als auch auf Landesebene existieren Listen über Risikogruppen, die teilweise laufend aktualisiert werden. Mithilfe solcher Listen (z.B. „Rocker", „Hooligans" oder „Rechtsradikale") können bspw. 200 Kennzeichen auf einmal in die Fahndungsdatei aufgenommen werden. Das System fahndet nach allen in die Suchdatei eingegebenen Kennzeichen gleichzeitig.*

**2.5** Welche Daten werden bei der automatischen Kennzeichenfahndung erhoben?

**a)** § 36a BbgPolG spricht nur von der Erhebung von „Kennzeichen". Das BVerfG weist aber darauf hin, dass in der Realität regelmäßig weitere Informationen erhoben werden. Welche Informationen werden im Trefferfall tatsächlich erhoben?

*Es werden das Kennzeichen-Bild als Konstrukt, ein Echtfoto, das Ausstellungsland des Kennzeichens, das Trefferdatum mit Uhrzeit, der Standort, eine interne Identifikationsnummer (ID) und der Status (Treffer) gespeichert.*

**b)** Was ist auf dem angefertigten Bild zu sehen? Können Fahrer und Beifahrer oder gar weitere Insassen erkannt und identifiziert werden?

*Das im Trefferfall angefertigte Bild erfasst das Auto von hinten, was praktische und taktische Gründe hat. Bspw. sind die hinteren Kennzeichen bei nassem Wetter in der Regel sauberer. Personen sind auf dem Bild nicht erkennbar. Bei dem Bild handelt es sich um eine Schwarz-Weiß-Aufnahme, auf der nur das die Kamera auslösende Kennzeichen deutlich erkennbar ist. Weitere Daten wie z.B. auf dem Fahrzeug aufgeklebte Autowerbung werden nicht erfasst.*

**c)** Kann die automatische Kennzeichenfahndung auch zur Suche von Motorrädern eingesetzt werden

*Da die gesuchten Fahrzeuge von hinten erfasst werden, können auch die Kennzeichen von Motorrädern ausgelesen werden. Die automatische Kennzeichenfahndung ist daher auch zur Fahndung nach Motorrädern einsetzbar.*

**d)** Welche Funktion hat das Bild? Dient es der manuellen Kontrolle oder als Beweismittel?

*In erster Linie dient das Bild dem manuellen Abgleich des Treffers mit dem Fahndungsbestand. Wie bereits erläutert wurde, zieht die Anwendungssoftware die Kennzeichen ja zusammen und erfasst keine Leerzeichen, Fremdkörper usw. In seltenen Fällen kann es daher vorkommen, dass die Kamera fehlerhaft ausgelöst wird. Wird z.B. nach dem Kennzeichen B-AX 1234 gefahndet, wandelt die Anwendungssoftware dieses Kennzeichen in BAX1234 um. Passiert das Kennzeichen BA-X 1234 nun die Kontrollanlage, wird ein Trefferfall gemeldet, der als Fehltreffer zu bewerten ist. Durch den manuellen Abgleich des Bildes mit dem Fahndungsbestand werden derartige Fehler ausgeglichen, bevor es zu einer weiteren Maßnahme kommt.*

**2.6** In der Regel erkennt der normale Bürger nicht, ob eine am Straßenrand aufgestellte Kamera der Geschwindigkeitskontrolle oder einer automatischen Kennzeichenfahndung dient. Handelt es sich bei der automatischen Kennzeichenfahndung schon deshalb um eine verdeckte Maßnahme? Müssten für eine offene Kennzeichenfahndung Schilder aufgestellt werden, die auf die Kennzeichenfahndung hinweisen?

*Nein. Eine verdeckte Maßnahme liegt nur dann vor, wenn das Instrumentarium von der Polizei bewusst verdeckt wird, wenn für den Bürger also nicht mehr erkennbar sein soll, dass eine polizeiliche Maßnahme durchgeführt wird.*

*Von einer offenen Maßnahme wird hingegen immer dann gesprochen, wenn für die Bürger ersichtlich ist, dass überhaupt irgendeine polizeiliche Maßnahme durchgeführt wird. Um welche Maßnahme es sich dabei genau handelt, muss für den Bürger nicht erkennbar sein.*

**2.7** Technische Durchführung

**a)** Was versteht man unter einem „stationären" Gerät, was unter einem mobilen Gerät?

*Stationäre Geräte sind fest mit dem Boden verbunden bzw. an Brücken fest installiert. Mobile Geräte kommen entweder aus dem Auto heraus zum Einsatz oder werden am Straßenrand aufgestellt.*

**b)** Wo findet der eigentliche Rechenvorgang statt? Gibt es ggf. einen landesweiten Zentralserver?

Ja, es gibt einen landesweiten Zentralserver, *der speziell für „Kesy" errichtet wurde. Die von den stationären Kontrollgeräten erfassten Kennzeichen werden an diesen Zentralserver übermittelt und dort abgeglichen. Liegt kein Treffer vor, werden die Daten von dem Server unverzüglich gelöscht. Sie können nicht rekonstruiert oder auf irgendeine Weise nachträglich eingesehen werden. Im Trefferfall hingegen werden die erfassten Daten vom Server an die Zentralstelle in Frankfurt / Oder weitergeleitet.*

*Beim Einsatz von mobilen Geräten werden die Kennzeichen vor Ort auf einem Laptop abgeglichen.*

**c)** Wie viele Kennzeichen kann ein Gerät, das für die automatische KF eingesetzt wird, pro Stunde erfassen und auswerten?

*Die Geräte können etwa 2 Kennzeichen pro Sekunde auslesen. Die Fehlerrate liegt bei ca. 4%. Als Ursache für die auftretenden Fehler sind v.a. die Verschmutzung von Kennzeichen oder die Abdeckung von Kennzeichen zu nennen.*

**d)** Werden bspw. auf Autobahnen alle Fahrspuren auf einmal erfasst? Erfasst das Gerät nur die Fahrzeuge in eine Richtung oder in beide Richtungen?

*Bei stationären Geräten können zwei Fahrspuren gleichzeitig erfasst werden.*

**e)** Wie leicht kann auf den Erfolg einer automatische Kennzeichenfahndung Einfluss genommen werden (z.B. durch das Aufkleben von reflektierender Folie)?

*Da die eingesetzten Geräte mit einer Infrarot-Technik arbeiten, hat das Aufkleben von reflektierender Folie keinen Einfluss auf den Erfolg der Maßnahme. Der Blitz ist für die Autofahrer nicht einmal erkennbar.*

**f)** Inwiefern beeinflussen die Witterungsverhältnisse das Ergebnis einer automatische Kennzeichenfahndung? Beeinträchtigen bspw. Regen und Nebel die automatische Kennzeichenfahndung?

*Die Durchführung einer automatischen Kennzeichenfahndung ist bei allen Wetterlagen möglich. Es hat sich sogar erwiesen: Je schlechter die Witterungsverhältnisse sind, desto besser sind die erzielten Bilder. Dies liegt daran, dass die automatische Kennzeichenfahndung mit Hilfe von Infrarot-Kameras erfolgt.*

**2.8** Ist es auch möglich, lediglich Kennzeichenfragmente in die Datenbank einzugeben?

*Ja. Auch diese Technik wird gelegentlich gezielt zur Gefahrenabwehr eingesetzt. Wird bspw. bei einem Fußballspiel mit massiven Ausschreitungen gerechnet, so kann z.B. lediglich HRO in die Datenbank eingegeben werden. Auf diese Weise wird in Erfahrung gebracht, wie viele Hansa-Rostock-Fans zu dem Fußballspiel z.B. in Cottbus anreisen und wie viele Polizeikräfte bei dem Fußballspiel bereitgestellt werden müssen.*

**3. Ortung von Mobiltelefonen** (§ 33b Abs. 3 Nr. 2 BbgPolG)

**3.1** Für welche Fallkonstellationen wurde die Handyortung konzipiert? Welche Situationen sind für den Einsatz dieser Maßnahme typisch?

*Die Handyortung wurde v.a. für die Suche nach vermissten Personen, Suizidgefährdeten und Demenzkranken konzipiert. Die Suche nach suizidgefährdeten Personen stellt mit über 50% den größten Anwendungsbereich der Handyortung dar. Auch im Fall eines angedrohten oder gerade stattfindenden Amoklaufs könnte eine Handyortung sinnvoll sein. Eine solche Situation ist in Brandenburg bisher jedoch nicht eingetreten, die Maßnahme wurde in diesem Zusammenhang bisher also noch nicht eingesetzt.*

**3.2** Welche Informationen (neben der Handynummer) sind für eine Handyortung notwendig?

*Für eine Handyortung benötigt die Polizei in erster Linie die IMSI-Nummer des gesuchten Handys und dessen Standortinformationen.*

**3.3** Wer führt die Handyortung durch? Die Polizei selbst mithilfe der IMSI-Catcher, oder bedient sich die Polizei der TK-Unternehmen, um den Standort eines Handys festzustellen? Welche Rolle spielt die Verkehrsdatenabfrage nach § 33b VI BbgPolG im Rahmen einer Handyortung?

*§ 33b III Nr. 2 BbgPolG und § 33b VI BbgPolG greifen ineinander. Der Rat vom Dienst (RvD) führt die Handyortung selbst durch. Allerdings benötigt er dazu diverse Daten von den Telekommunikationsunternehmen. Insbesondere müssen die TK-Unternehmen dem Rat vom Dienst (RvD) mitteilen,*

- *ob das Handy der Zielperson eingeschaltet ist*
- *in welcher Funkzelle*
- *und in welcher Geokoordinate es sich befindet*
- *den CI und*
- *den Location Area Code (LAC), eine Angabe, die den Bereich eingrenzt, in welchem sich das Handy befindet (Großraumbereich, vgl. Postleitzahl).*

*Erst wenn bekannt ist, in welcher Funkzelle sich das gesuchte Handy befindet, kommt der IMSI-Catcher zum Einsatz. Auf diese Weise wird der Aufenthaltsort des gesuchten Handys weiter eingegrenzt. Ist der ungefähre Aufenthaltsort der Zielperson bekannt, wird zur Feinlokalisierung ein Handpeiler eingesetzt, der den genauen Standort des gesuchten Mobiltelefons ermittelt.*

**3.4** Wie lange dauert die Ortung eines Mobiltelefons erfahrungsgemäß?

*Das hängt sehr von der Größe der Funkzellen ab. Innerstädtisch ist die Maßnahme i.d.R. nach max. 1 Std. abgeschlossen. Auf dem Land dauert sie viel länger, gerne auch einmal 10 Stunden.*

**3.5.** Wie viele IMSI-Catcher gibt es in Brandenburg, und wo befinden sich diese?

*In Brandenburg gibt es lediglich einen IMSI-Catcher. Dieser befindet sich beim LKA. Er ist nur fahrzeuggebunden einsetzbar, was z.B. in Bahnhofsgebäuden problematisch sein kann. Allerdings ist es möglich, einen Teil des Gerätes aus dem Fahrzeug herauszunehmen und herumzutragen.*

*Das Polizeipräsidium besitzt keinen eigenen IMSI-Catcher. Eine Anfrage beim LKA wird nur selten gestellt, i.d.R. sucht das Polizeipräsidium nach einer Zellabfrage bei den TK-Unternehmen mit Personenkraft, Hubschrauber usw. nach der Zielperson.*

**3.6** Wie genau ist eine Lokalisierung möglich? Angenommen es findet ein Amoklauf statt: Kann lediglich bestimmt werden, in welchem Gebäude sich der Täter befindet oder auch in welchem Gebäudeflügel oder gar in welchem Zimmer?

*Grundsätzlich ist eine sehr genaue Ortung möglich, unter gewissen Umständen kann jedoch nur der ungefähre Standort ermittelt werden.*

**3.7** Was versteht man unter einer sog. „stillen SMS" und dem sog. „Pingen"?

*Pingen bedeutet, dass ein Anruf simuliert wird. Der IMSI-Catcher stellt mit dem Zieltelefon eine Sprechverbindung her, die für den Gesuchten unmerklich ist. Der simulierte Anruf wird nur im Catcher angezeigt. Ansonsten ist er nirgendwo und niemandem ersichtlich, nicht einmal im Rahmen einer TKÜ/VDÜ wird er angezeigt.*

*Eine „stille SMS" dient nur der Ermittlung von Geo-Koordinaten. Sie wird auf dem Zieltelefon nicht angezeigt, i.Ü. wird sie aber wie eine normale SMS erfasst. So wird sie bspw. i.R. einer TKÜ/VDÜ angezeigt.*

**3.8** Werden durch die Handyortung die Einsatzbereitschaft oder die Funktionsfähigkeit des gesuchten Handys oder gar aller im Bereich der Funkzelle liegenden Handys für einen Augenblick beeinträchtigt?

*Nein. Der IMSI-Catcher stellt zu dem gesuchten Mobiltelefon eine Sprechverbindung her, die für den Gesuchten unmerklich ist. Er simuliert eine Funkzelle, die stärker ist als die Serverzelle. Die Ummeldung in diese neue, simulierte Zelle – die sog. „blind cell" – dauert 800 ms.*

**3.9** Können mit Hilfe des IMSI-Catchers nur gezielt nach einer oder auch gleichzeitig nach mehreren Nummern gesucht werden? Wäre es auch denkbar, mithilfe des IMSI-Catchers eine Suchaktion nach ganzen Tätergruppen durchzuführen (vgl. automatische Kennzeichenfahndung)?

*Theoretisch wäre es möglich, dass bspw. vor einem Fußballspiel tausende von Handys gleichzeitig geortet werden – vorausgesetzt, der Polizei sind alle IMSI-Nummern bekannt. Auch dann würde der IMSI-Catcher eine simulierte Funkzelle schalten und beim Passieren eines jeden gesuchten Handys ein Signal bei der Polizei auslösen. Diese Methode wird jedoch nicht praktiziert. Es wird immer nur ein Handy auf einmal geortet.*

**3.10** Ist die Erstellung von Bewegungsbildern in Echtzeit (≠ Bewegungsprofil) möglich?

*Die Erstellung von Bewegungsbildern in Echtzeit ist mit den vorhandenen technischen Mitteln nicht möglich. Die Verkehrsdaten, die bei den TK-Unternehmen abgefragt werden können, geben nur die Zelle an, in der sich das gesuchte Mobiltelefon befindet. Diese Daten sind also zu ungenau, um ein Bewegungsbild zu erstellen. Der IMSI-Catcher muss für jede einzelne Ortung eine neue Verbindung zu dem gesuchten Mobiltelefon herstellen. Aus diesem Grund können nur zahlreiche punktuelle Standortbestimmungen erfolgen, nicht aber die Erstellung eines Bewegungsbildes.*

*Bewegt sich die Zielperson mit ihrem Handy fort, wird gleichzeitig mit der zur Ortung erforderlichen Standortdatenabfrage nach § 33b VI BbgPolG eine TKÜ nach § 33b I BbgPolG beantragt, welche wiederum die „Verfolgung" der Zielperson ermöglicht.*

*Die Erstellung von Bewegungsbildern in Echtzeit ist zur Gefahrenabwehr nicht zulässig. Zu repressiven Zwecken wäre sie aus rechtlicher Sicht zwar theoretisch möglich, wird in der Praxis aber nicht durchgeführt.*

**3.11** Gibt es eine Möglichkeit, Verbindungsdaten oder die Daten, die zur Handyortung erforderlich sind, zu anonymisieren (vgl. Anonymisierungsdienste im Internet)?

*Nein. Es gibt keine Möglichkeit, irgendwelche Daten vor der Polizei zu „verstecken".*

**3.12** Bestands- und Verkehrsdaten müssen von allen Anbietern gespeichert werden. Werden auch Standortdaten eines Handys im Standby-Betrieb automatisch gespeichert?

*Nein, Standortdaten werden nur bei Aktivität des Handys gespeichert, also nur wenn eine SMS gesendet, empfangen oder ein Telefonat geführt wird.*

**4. Verkehrsdatenabfrage** (§ 33b VI 2 BbgPolG)

**4.1** Für welche Fallkonstellationen wurde die Verkehrsdatenabfrage konzipiert? Welche Situationen sind für den Einsatz dieser Maßnahme typisch?

*Im präventiven Einsatzbereich hat die Verkehrsdatenabfrage in aller Regel eine reine (technische) Hilfsfunktion.*

**4.2** Wie lange dauert es i.d.R., bis die TKU die Verkehrsdaten zur Verfügung stellen?

*I.d.R. wird der Antrag der Polizei auf Erteilung der Verkehrsdaten per Fax an die TKU übermittelt. Diese führen keine rechtliche Prüfung des Antrages durch, sondern übermitteln die angeforderten Daten ohne weitere Prüfung ebenfalls per Telefax an die entsprechende Polizeidienststelle. Diese Vorgehensweise ermöglicht eine sehr schnelle Verfügbarkeit der Verkehrsdaten.*

**4.3** Spielt es bei der Überlegung und der Entscheidung über die Anforderung von Verkehrsdaten eine Rolle, dass den TKU die Kosten für ihr Tätigwerden ersetzt werden müssen? Gibt es Haushaltsvorgaben oder gar eine Sperre bei ausgeschöpftem Budget?

*Nein. Über die Kostenerstattungspflicht wird bei der Entscheidung über den Einsatz einer derartigen Maßnahme nicht nachgedacht. Sofern eine Maßnahme nach einer pflichtbewussten Prüfung der vorhandenen Möglichkeiten erforderlich erscheint, wird sie durchgeführt – auch am Ende eines Haushaltsjahres. Eine Verkehrsdatenabfrage kostet 90,- €, das An- und Ausschalten einer TKÜ 170,- €. An- und Ausschalten einer TKÜ bedeutet dabei, dass die TK-Unternehmen lediglich die Leitung zur Polizei durchschalten. Die eigentliche TKÜ führt die Polizei daraufhin selbst durch.*

## 3. Variablenplan

### 1. Verfahrensdaten

1.1 Aktenzeichen Behörde
1.2 Datum Antrag
1.3 Uhrzeit Antrag
1.4 Datum Anordnung
1.5 Uhrzeit Anordnung
1.6 Datum Einsatz (Beginn)
1.7 Uhrzeit Einsatz (Beginn)
1.8 geplante Dauer d. Maßnahme
1.9 Datum Einsatz (Ende)
1.10 Uhrzeit Einsatz (Ende)
1.11 tatsächliche Dauer (h)
1.12 Datum Verfahrensabschluss
1.13 Unterbrechungen
1.14 Wiederholungen
1.15 Zielsetzung
- 01 präventiv
- 02 repressiv
- 03 doppelfunktional

### 2. Beteiligte Behörden

2.1 antragstellende Behörde
- 01 Gericht
- 02 StA
- 03 Innen-/Justizministerium
- 04 LKA
- 05 Polizeipräsidium
- 06 untergeordnete Behörde
- 07 Amtshilfe

2.2 anordnende Behörde
- 01 Gericht
- 02 StA
- 03 Innen-/Justizministerium
- 04 LKA
- 05 Polizeipräsidium
- 06 untergeordnete Behörde

2.3 TKÜ: Gericht
- 01 anordnend
- 02 nein, mgls. Erforderlichkeit
- 03 nein; Gefahr im Verzug

2.4 durchführende Behörde
- 01 LKA
- 02 Polizeipräsidium
- 03 untergeordnete Behörde

2.5 TKÜ: richterliche Anordnung nachträglich eingeholt? (ja/nein)

## 3. Hintergrund

3.1 Anlass*
- 01 Gefahr für Leib
- 02 Gefahr für Leben
- 03 Gefahr für Freiheit
- 04 sonstige Gefahr
- 05 Tötungsdelikt
- 06 Körperverletzungsdelikt
- 07 Eigentumsdelikt
- 08 Sachbeschädigungsdelikt
- 09 BtMG-Delikt
- 10 Staatsschutzdelikt
- 11 sonstiges Delikt
- 12 polizeiliche Ausschreibung

3.2 Straftat Deliktstyp
- 01 Tötungsdelikt
- 02 Körperverletzungsdelikt
- 03 Eigentumsdelikt
- 04 Sachbeschädigungsdelikt
- 05 BtMG-Delikt
- 06 Staatsschutzdelikt
- 07 sonstiges Delikt

3.3 vorausgegangene Maßn./ Datum

3.4 vorausgeg. Maßn. / Details*
- 01 Personenfeststellung
- 02 erkennungsdienstl. Maßn.
- 03 Vorladung / Vernehmung
- 04 Durchsuchung von Personen, Sachen oder Wohnungen
- 05 Sicherstellung, Beschlagnahme, Einziehung
- 06 sonstige
- 07 vorherige Anhörung erfolgt

3.5 ursprüngl. Informationsquelle*
- 01 Anzeige durch Private
- 02 Anzeige durch Behörde
- 03 V-Mann / Informant
- 04 Polizeitätigkeit / eigene Ermittlungen

3.6 Begründung Antrag
- 01 allgemein
- 02 detailliert

3.7 Begründung Anordnung
- 01 allgemein
- 02 detailliert

3.8 Umfang Begründung Antrag (S.)

3.9 Umfang Begr. Anordnung (S.)

3.10 Umfang Einsatzprotokoll (S.)

3.11 Umfang Akte insgesamt (S.)

**4. beteiligte Personen**

4.1 Zielperson des Verfahrens
- 01 Störer / Beschuldigter
- 02 Teilnehmer / Kontakt- / Begleitperson
- 03 Gefährdeter / Opfer
- 04 Notstandspflichtiger / Dritter

4.2 Zielperson konkreter Einsatz
- 01 Störer / Beschuldigter
- 02 Teilnehmer / Kontakt- / Begleitperson
- 03 Gefährdeter / Opfer
- 04 Notstandspflichtiger / Dritter

4.3 Störer / Beschuldigter
- 4.3.1 Anzahl
- 4.3.2 Nummer
- 4.3.3 Alter
- 4.3.4 Geschlecht
  - 01 männlich
  - 02 weiblich
- 4.3.5 Staatsangehörigkeit
- 4.3.6 Wohnort
- 4.3.7 Anzahl Vorstrafen
- 4.3.8 Art der Vorstrafen
- 4.3.9 Vorstrafen in Begründung thematisiert?

4.4 Teilnehmer / Kontakt- / Begleitperson
- 4.4.1 Anzahl
- 4.4.2 Nummer
- 4.4.3 Alter
- 4.4.4 Geschlecht
  - 01 männlich
  - 02 weiblich
- 4.4.5 Staatsangehörigkeit
- 4.4.6 Wohnort
- 4.4.7 Tatbeitrag
- 4.4.8 Anzahl Vorstrafen
- 4.4.9 Art der Vorstrafen
- 4.4.10 Vorstrafen in Begründung thematisiert?

4.5 Gefährdeter / Opfer
- 4.5.1 Anzahl
- 4.5.2 Nummer
- 4.5.3 Alter
- 4.5.4 Geschlecht
  - 01 männlich
  - 02 weiblich
- 4.5.5 Staatsangehörigkeit

4.6 Notstandspflichtiger / Dritter
- 4.6.1 Anzahl
- 4.6.2 Nummer
- 4.6.3 Alter
- 4.6.4 Geschlecht
  - 01 männlich
  - 02 weiblich
- 4.6.5 Staatsangehörigkeit
- 4.6.6 bewusst und gezielt miterfasst? (ja/nein)
- 4.6.7 Betroffenheit unvermeidbar? (ja/nein)
- 4.6.8 Grund für Inanspruchnahme

## 5. Autom. Kennzeichenfahndung

| | |
|---|---|
| 5.1 | Fahndungsgegenstand* |
| | 01 Auto |
| | 02 Motorrad |
| | 03 sonstiges |
| 5.2 | Vorgehensweise* |
| | 01 offen |
| | 02 verdeckt |
| | 03 stationär |
| | 04 mobil |
| | 05 halb-stationär |
| 5.3 | Anzahl eingesetzter Systeme |
| 5.4 | Personalaufwand vor Ort |
| 5.5 | Inhalt der Fahndungsdatei (Anzahl eingegebener Kennzeichen) |
| 5.6 | Kennzeichen in anderer Fahndungsdatei enthalten? (ja/nein) |
| 5.7 | Anzahl Treffermeldungen |
| 5.8 | tatsächliche Treffer |
| 5.9 | Fehltreffer |
| 5.10 | Trefferquote (%) |
| 5.11 | auf dem Bild erkennbar* |
| | 01 Kennzeichen |
| | 02 Fahrzeugtyp |
| | 03 Farbe |
| | 04 Insassen |
| | 05 sonstiges |

## 6. Verkehrsdatenabfrage

6.1 Abfrage bei folgenden TKU*:
- 01 D1 / T-Mobile / Telekom
- 02 D2 / Vodafone
- 03 O2
- 04 E-Plus
- 05 Arcor
- 06 1&1
- 07 Versatel
- 08 Freenet
- 09 Sonstige

6.2 Anzahl abgefragter Anschlüsse

6.3 Auskunft durch TKU erteilt?
- 01 ja, alle
- 02 teilweise
- 03 nein

6.4 Treffer bei folgenden TKU*:
- 01 D1 / T-Mobile / Telekom
- 02 D2 / Vodafone
- 03 O2
- 04 E-Plus
- 05 Arcor
- 06 1&1
- 07 Versatel
- 08 Freenet
- 09 Sonstige

6.5 Abfrageform*
- 01 gewählte Nummern
- 02 Zielsuchlauf
- 03 Zellinformationen
- 03 vorhandene Daten
- 04 zukünftige Daten

6.6 Ortung als Anschlussmaßnahme? (ja/nein)

6.7 Kosten VDA (€)

6.8 Vernichtung der erlangten Daten nach Verfahrensabschluss? (ja/nein)

6.9 zeugnisverweigerungsberechtigte Personen betroffen? (ja/nein)

6.10 war Zeugnisverweigerungsrecht vorher bekannt?

## 7. Ortung

7.1 angestrebter Zweck der Ortung*
- 01 Standort e. Person ermitteln
- 02 Daten eines Mobiltelefons ermitteln
- 03 sonstiges

7.2 Dauer erster Einsatz des IMSI-Catchers bis Zweckerreichung

7.3 Personalaufwand

7.4 Erlangung der für die Ortung erforderlichen Daten*
- 01 durch Privatperson / Anzeige
- 02 durch Verkehrsdatenabfrage (inkl. Funkzellenabfrage)
- 03 durch Einsatz des IMSI-Catchers
- 04 sonstiges

7.5 Kosten der Ortung (€)

**8. weiteres Verfahren / Ergebnisse**

8.1 parallel stattfindende Maßnahmen

8.2 Anschlussmaßnahmen*
- 01 keine
- 02 Verfolgung
- 03 Festnahme
- 04 Personenfeststellung
- 05 erkennungsdienstliche Maßnahmen
- 06 Vorladung, Vernehmung
- 07 Durchsuchung von Personen, Sachen oder Wohnungen
- 08 Sicherstellung, Beschlagnahme, Einziehung
- 09 Rettungsmaßnahmen
- 10 Sonstige
- 11 verdeckte Anschlussmaßnahmen

8.3 Effizienz des Einsatzes
- 01 unmittelbarer Erfolg (Gefahr / Straftat abgewandt / Beschuldigter gefasst)
- 02 mittelbarer Erfolg / Anschlussmaßnahmen ermöglicht)
- 03 erfolglos (Gefahr verwirklicht / Straftat begangen / Straftat nicht aufgeklärt)

8.4 präventiver Einsatz: eingetretener Schaden*
- 01 Personenschaden entspr. Gefahr
- 02 abweichender Personenschaden
- 03 Körperverletzung
- 04 Tötung
- 05 Sachschaden entspr. Gefahr
- 06 abweichender Sachschaden

8.5 präventiver Einsatz: Höhe des eingetretenen Sachschadens

8.6 präventiver Einsatz: weiteres Verfahren der Polizei
- 01 Erledigung
- 02 Einstellung
- 03 Fortführung / Abschluss durch Polizei
- 04 Weiterleitung an StA

8.7 präventiver Einsatz: Datum Akteneingang bei der StA

8.8 weiteres Verfahren der StA
- 01 Erledigung
- 02 Einstellung nach § 153 I
- 03 Einstellung nach § 153a I
- 04 Einstellung nach § 153b I
- 05 Einstellung nach § 154
- 06 sonstige Einstellung
- 07 Klageerhebung
- 08 sonstiges

8.9 Akteneingang bei Gericht

8.10 weiteres Verfahren des Gerichts
- 01 Einstellung nach § 153 II
- 02 Einstellung nach § 153a II
- 03 Einstellung nach § 153b II
- 04 Einstellung nach § 154
- 05 sonstige Einstellung
- 06 Eröffnung / Hauptverhandl.

8.11 Anzahl der Instanzen

8.12 Hauptentscheidung*
01 Freispruch
02 Geldstrafe / Geldbuße
03 Freiheitsstrafe
04 sonstiges

8.13 Nebenentscheidungen

8.14 rechtliche Bewertung der Tat*
gem. justizieller (in Rechtskraft erwachsender) Entscheidung
01 Tötungsdelikt
02 Körperverletzungsdelikt
03 KfZ-Diebstahl
04 sonstiges Eigentumsdelikt
05 Sachbeschädigungsdelikt
06 BtMG-Delikt
07 Staatsschutzdelikt
08 sonstige Straftat
09 Ordnungswidrigkeit

8.15 rechtliche Bewertung (§§)

8.16 Verwertung durch die Maßnahme gewonnenen Erkenntnisse im weiteren Verfahren*
01 i.R.d. staatsanwaltlichen Ermittlungstätigkeit
02 im gerichtlichen Verfahren
03 das Urteil wurde auf die durch die Maßnahme erlangten Erkenntnisse gestützt
04 das Urteil wurde auf Erkenntnisse aus Anschlussmaßnahmen gestützt

**9. Anmerkungen**

* Mehrfachnennung möglich

LAND BRANDENBURG

Ministerium des Innern

Ministerium des Innern des Landes Brandenburg | Postfach 601165 | 14411 Potsdam

Henning-von-Tresckow-Straße 9-13
14467 Potsdam

Bearb.: Herr Gerner
Gesch.Z.: IV/1.1. - 420 - 44
Hausruf: (0331) 866 2894
Fax: (0331) 866 2402
Internet: www.mi.brandenburg.de
Karlheinz.Gerner@mi.brandenburg.de

Bus: 695; Tram: 91, 92, 93, 96, X98, 99
Zug: RE 1, RB 20, RB 21, RB 22; S-Bahn: S7

Polizeipräsidium Frankfurt (Oder)

Polizeipräsidium Potsdam

Landeskriminalamt Brandenburg

Zentraldienst der Polizei

Landeseinsatzeinheit

Fachhochschule der Polizei

Potsdam, den 14. Juli 2010

**Auslegung des § 33b Absatz 6 Satz 2 BbgPolG**

Durch das Urteil des Bundesverfassungsgerichts vom 2. März 2010 zur Vorratsdatenspeicherung (BVerfG, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08) wurden die §§ 113a, 113b TKG für nichtig erklärt. Ferner wurde § 100g StPO insoweit für nichtig erklärt, als danach Telekommunikationsverkehrsdaten nach § 113a TKG erhoben werden dürfen. Die aufgrund einstweiliger Anordnungen des Bundesverfassungsgerichts, insbesondere die aufgrund der einstweiligen Anordnung vom 11. März 2008, erhobenen Telekommunikationsdaten sind unverzüglich zu löschen und dürfen nicht an ersuchende Stellen übermittelt werden.

In Auswertung des o. g. Urteils gebe ich zur Auslegung des § 33b Absatz 6 Satz 2 BbgPolG folgende Hinweise:

1. Polizeiliche Auskunftsersuchen gemäß § 33b Absatz 6 Satz 2 BbgPolG können auch weiterhin auf Telekommunikationsverkehrsdaten im Sinne des § 96 Absatz 1 TKG gerichtet sein.

2. Abweichend von der hier bislang vertretenen Rechtsauffassung und entsprechend der zum Teil bereits geübten Praxis sind Auskunftsersuchen gemäß § 33b Absatz 6 Satz 2 BbgPolG gegenüber Diensteanbietern bezüglich gespeicherter Telekommunikationsverkehrsdaten im Sinne des § 96 Absatz 1 TKG grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen.

3. Zuständig ist das Amtsgericht, in dessen Bezirk die beantragende Polizeibehörde ihren Sitz hat.

4. Die Anordnung der Abfrage von Telekommunikationsverkehrsdaten durch einen Richter im Rahmen des § 33b Absatz 6 Satz 2 BbgPolG ist bei Gefahr im Verzug nicht erforderlich. Gefahr im Verzug liegt vor, wenn die richterliche Anordnung „ohne Gefährdung des Zwecks" der Maßnahme „nicht rechtzeitig erlangt werden kann" (vgl. OVG Berlin-Brandenburg, Beschluss vom 1. Sept. 2009 – OVG 1 L 100.8); sie liegt – umgekehrt – nicht vor, wenn „für die Einholung einer richterlichen Entscheidung ... angesichts der Vorbereitung der Polizeiaktion ... ausreichend Zeit" ist (vgl. OVG Berlin-Brandenburg, Urteil vom 10. Sept. 2009 – OVG 1 B 29.09). Bei Gefahr im Verzug kann der Behördenleiter, im Falle seiner Verhinderung sein Vertreter im Amt, die Abfrage von Telekommunikationsverkehrsdaten anordnen; in diesem Fall ist unverzüglich eine richterliche Bestätigung einzuholen.

5. In allen anderen Fällen, insbesondere bei der vorbeugenden Bekämpfung von Straftaten bleibt es beim Erfordernis einer richterlichen Anordnung.

Das Bundesverfassungsgericht verlangt zur Sicherung eines effektiven Rechtsschutzes, dass eine Abfrage oder Übermittlung von Telekommunikationsverkehrsdaten grundsätzlich unter Richtervorbehalt zu stellen ist. Das o. g. Urteil betrifft nicht unmittelbar die nach § 96 Absatz 1 TKG gespeicherten Daten. Da diese jedoch teilidentisch mit zuvor nach § 113a TKG gespeicherten Telekommunikationsverkehrsdaten sind, ist von einer vergleichbaren Datensensibilität und Eingriffsintensität auszugehen und im Ergebnis § 33b Absatz 6 Satz 2 BbgPolG dahingehend auszulegen, dass eine entsprechende Anfrage in Bezug auf Telekom-

munikationsverkehrsdaten gemäß § 96 Absatz 1 TKG grundsätzlich unter Richtervorbehalt stehen muss. Ungeachtet dessen kann aber nach Nr. 4 insbesondere in den Fällen der

- Beseitigung einer Suizidgefahr,
- Suche nach gefährdeten Vermissten,
- Suche nach minderjährigen Vermissten oder
- Befreiung aus hilfloser Lage (z.B. im Wald verirrte Person)

eine 'Gefahr im Verzug' vorliegen, weil aufgrund der Prüfung im Einzelfall die Zeit fehlt, vor dem Auskunftsersuchen einen Richter zu erreichen. Dann ist die richterliche Entscheidung unverzüglich nachzuholen.

Im Auftrag

Gehne