Ulrike Donat
Rechtsanwältin
Kaiser-Wilhelm-Str. 93 VI
20355 Hamburg
Tel. 040 - 42289 3830
Fax: 040 - 41189 3837
kontakt@ulrike-donat.de
www.ulrike-donat.de

Zur Renovierungsbedürftigkeit des Hamburger Polizeirechtes

Gutachten unter besonderer Berücksichtigung der jüngeren Rechtsprechung des Bundesverfassungsgerichtes zu polizeilichen Überwachungsmaßnahmen

Inhaltsverzeichnis

Die Änderungen im Landes- und Bundespolizeirecht der vergangenen Jahre haben die rechtliche Landschaft vollständig verändert. Unter der Überschrift „Sicherheit statt Freiheit“ wurden Polizeibefugnisse auf Bundesebene ebenso ausgebaut, wie bürgerliche Freiheitsrechte im Landespolizeirecht und Bundespolizeirecht beschnitten. Immer neue „Sicherheitstechnik“ erfordert immer wieder neue Eingriffsbefugnisse. Die Evaluierung von Nutzen und Schaden der neuen Überwachungstechnik fehlt weitgehend.

Das Bundesverfassungsgericht hat eine Reihe von Entscheidungen zu polizeilichen Eingriffs-, Vorfeld- und Überwachungsmaßnahmen getroffen, die eine rechtliche Überprüfung der jüngeren Änderungen des Hamburger Polizeirechtes erfordern.

Dies ist Gegenstand des nachfolgenden Gutachtens.

Die Forderung nach Begrenzung und Kontrollierbarkeit polizeilicher Macht ist Folge und Auftrag der Deutschen Geschichte. Die „klassischen“ Anforderungen an rechtmäßiges Polizeihandeln beruhen auf der Erfahrung zunächst mit dem Obrigkeitsstaat, dann mit Diktaturen in Deutschland. Die Begrenzungen polizeilicher Macht dienen nicht der Behinderung der Polizeiarbeit oder der Verhinderung von Sicherheit, sondern sollen ein ausgewogenes Verhältnis zwischen den Notwendigkeiten eines geordneten und sicheren Zusammenlebens einerseits, der Bewahrung der Freiheitsrechte und der Würde des Einzelnen andererseits sicherstellen.

1 Das „klassische Instrumentarium“ des Polizeirechtes und das „neue Sicherheitsrecht“

Unter der Geltung des Grundgesetzes gibt es einige bislang selbstverständliche Grundsätze des Polizeirechtes, die unter der neuen Sicherheitsphilosophie relativiert werden. Diskussionsbedürftig sind die Grenzen dieser Relativierung. Neue Informationstechnik verändert die Sicherheitslandschaft ebenso, wie die Föderalismusreform, die Europäisierung des Polizeirechtes und die Einbindung Privater in Sicherheitsaufgaben. Diese Entwicklung wird in der Fachliteratur und in der Öffentlichkeit seit längerem kritisch kommentiert.[1]

1.1 Klassisches Polizeirecht

Polizeiliche Eingriffe beschränken verfassungsrechtlich garantierte Freiheitsrechte und brauchen daher immer eine **gesetzliche Ermächtigung**. Diese muß Eingriffsbefugnisse fixieren und die Beachtung der Verhältnismäßigkeit **(**Erforderlichkeit und Geeignetheit der Maßnahme, Verhältnismäßigkeit im engeren Sinne) sowie des Wesensgehaltes der Freiheitsgrundrechte und der Menschenwürde des Grundgesetzes

[1] z. B. Kutscha/ Roggan (Hrsg.), Handbuch zum Recht der Inneren Sicherheit, 2. Aufl. 2006; Lisken/Denninger in Lisken/Denninger, Handbuch des Polizeirechtes, 4. Aufl. 2007, Kap C;

sicherstellen. Dafür muß die gesetzliche Ermächtigung **methodisch klar und übersichtlich** gefaßt werden, denn

- Bürger müssen sich auf eine etwaige Polizeipflicht oder sonstige Inanspruchnahme einstellen können
- Bürger müssen sich der polizeilichen Überwachung zum Erhalt ihrer Intim- und Freiheitssphäre entziehen können
- Polizeibeamte müssen die Grenzen ihrer Befugnisse erkennen und verstehen können
- Polizeiarbeit muß kontrollierbar sein
    - durch die Gerichte
    - durch das Parlament
    - und durch die Öffentlichkeit

Wesentliche Entscheidungen der Freiheitsbegrenzung müssen vom **Gesetzgeber** getroffen werden und dürfen nicht der Interpretation der Exekutive überlassen werden. Eingriffsakte müssen **justiziabel** sein. Bürger müssen Beschränkungen nur hinnehmen zum Schutz gleichwertiger oder höherrangiger Rechtsgüter, jede Einschränkung muß gemessen am Zweck und Intensität des Eingriffs **verhältnismäßig** sein. Sie finden ihre absolute Grenze in der Wahrung der **Menschenwürde.**

1.2 Neues Sicherheitsrecht

Das „neue“ Sicherheitsrecht vollzieht gegenüber diesen Traditionen einen Wandel und hebelt die eben genannten traditionellen Begrenzungsmechanismen im Polizeirecht - ersatzlos - aus, z.B. durch:

- „**Jedermann“-Eingriffe** statt Störerverantwortlichkeit
    - **verdachts- und gefahrunabhängig** (z.B. Raster- und Schleierfahndung)
    - mit **Ortsanknüpfung** statt Personenverantwortlichkeit (z.B. Videoüberwachung, Kontrollstellen)
- Einbeziehung von **Kontaktpersonen und Unbeteiligten** statt Beschränkung auf Störer/Nichtstörer nur im Notstandsfall
- **Heimlichkeit** statt offener Inanspruchnahme mit der Folge begrenzter Rechtsschutzmöglichkeiten und Leerlaufen der „Grundrechtssicherung durch Verfahrensgarantien“
- anlaßunabhängige **Vorfeldeingriffe** statt Eingreifen erst bei konkreter unmittelbarer Gefahr oder verdichtetem Tatverdacht
- umfangreicher Einsatz moderner Überwachungstechnik
- Datenverwendungsmöglichkeiten mit der Möglichkeit umfassender **Persönlichkeits- und Bewegungsprofile**

1.3 Neue Sicherheitstechnik

Neue Technik erlaubt in bislang ungekanntem Ausmaß die digitale Datenverarbeitung mit einer Potenzierung der speicherbaren verknüpfungsfähigen persönlichen Daten. Zusammen mit der Ausweitung verdachtsunabhängiger Vorfeldbefugnisse

ergeben sich weitere Probleme für den Grundrechtsschutz und die Verhältnismäßigkeit von Maßnahmen, insbesondere auch bei Speicherung, Verarbeitung, Abgleich, Abruf und Übermittlung von Daten durch

- die sog. **„Streubreite“** der Datenerhebung bei Unbeteiligten
- Steigerung der **Eingriffsintensität** eigentlich „harmloser“ Eingriffe durch potentiell unbegrenzte Verwendungsmöglichkeiten der daraus gewonnenen Daten bis hin zu **„Bewegungsprofilen“**
- Steigerung der Eingriffsintensität durch **Aufweichung der Zweckbindung** bei der Verarbeitung von persönlichen Daten
- Verletzung der Vertraulichkeit der Kommunikation im Privatbereich und in Berufen, die auf Vertraulichkeit angewiesen sind
- Verknüpfuntsmöglichkeiten der Datenbestände verschiedener Behörden untereinander und mit privaten Unternehmen

Der wechselseitige Datenaustausch unterläuft die Begrenzungsfunktion der Zweckbindung von Daten im Datenschutzrecht. Die Ausdehnung heimlicher Datenerhebung macht Kontrolle und Rechtsschutz unmöglich. Das wechselseitige Zusammenführen von Datenbeständen schafft den „Gläsernen Menschen“ und die Möglichkeit von „Bewegungsprofilen“.

Hinzu kommt die zunehmende **digitale Erfassung der Bürger** auch in anderen Bereichen als dem Sicherheitsrecht, etwa durch die elektronische Gesundheitskarte, die Steuer-Identifikationsnummer und im Privatrecht durch die Erfassung von Kundendaten. Alle diese Daten können verknüpft werden, der Mensch erhält eine digitale statt personale Identität.

Die Erweiterung der Datenerhebungs- und Verwendungsbefugnisse ist zudem bedenklich, weil - etwa bei der Bestimmung „gefährlicher Orte“, „terrorismusverdächtiger Handlungen“ oder den Erfassungskriterien bei der Rasterfahndung - diskriminierende **Feindbilder** der Polizei ein gefährliches Eigenleben entwickeln und die verfassungsrechtlichen und gesetzlichen **Diskriminierungsverbote** aushebeln, etwa durch Anknüpfung an Religionszugehörigkeit, Herkunft etc.

1.4 Neue Aufgabenverteilung Bund - Land- Verfassungsschutz

Auch das Umfeld des Landespolizeirechtes hat sich vollständig verändert durch die **neue „Sicherheitsarchitektur“** nach 2001 und durch die Föderalismusreform:

Die Befugnisse der Bundespolizeibehörden (BKA, Bundespolizei, BfV, MAD, BND) wurden erweitert mit den Terrorismusbekämpfungsgesetzen 2001 (sog. „Otto-Katalog I und II) und erneut 2007. Alle Sicherheitsbehörde erhielten wechselseitig den Zugriff auf gespeicherte Daten. Die Sicherheitsüberprüfung auch für private Firmen wurde eingeführt sowie biometrische Paßdaten. Flankiert wurde der Ausbau der Bundeskompetenz im Polizeirecht durch Datenvernetzung u.a. nach dem Allgemeinen Terror-Datei-Gesetz (ATDG) 2006, aber auch Verbund- und Abrufdateien der Bundes- und Landespolizeibehörden sowie der Verfassungsschutzbehörden und Geheimdienste, ergänzt um neue Befugnisse wie Vorratsdatenspeicherung, Online-Durchsuchung, Zentralregister für biometrische Daten, Zweckänderung von Daten etc. Hinzu kommt der Aufbau des Gemeinsamen Terrorabwehrzentrums seit 2004, die Bundespolizeireform, das neue BKA-Gesetz, das Nationale Lage- und Sicher-

heitszentrum in Zusammenarbeit von Polizei und Militär sowie die Diskussion um den Inlandseinsatz der Bundeswehr.

Mit dieser Entwicklung ist die **Machtkontrolle durch horizontale und vertikale Gewaltenteilung**, nämlich durch die Landespolizeihoheit sowie die **Trennungsgebote** zwischen Polizei und Geheimdiensten einerseits, zwischen Polizei und Militär andererseits, grundlegend in Frage gestellt. In vielen Bereichen - wie etwa bei Terrorverdacht, aber auch bei politischen Protesten zum G 8, gegen Atomkraft, gegen Grüne Gentechnik u.a. - machen Bürgerinnen und Bürger die Erfahrung, daß auch die Machtkontrolle durch die Gewaltenteilung Legislative - Exekutive - Judikative nicht mehr zufriedenstellend funktioniert. Polizeiliche Eingriffsbefugnisse sind schwammig oder ausufernd formuliert, so daß sie ihre Begrenzungsfunktion verlieren und die Definitionsmacht einseitig zur Polizei verlagert wird. Rechtsschutz gegen polizeiliche Gefahrenprognosen - etwa bei Versammlungsverboten, Aufenthaltsverboten, Platzverweisen, Überwachungsmaßnahmen - erweist sich in der Praxis als kaum durchführbar. Insbesondere die erhobenen Daten verbreiten sich schneller, als die Bürger Rechtsschutz erlangen können. Alternative Mechanismen der Kontrolle polizeilicher Allmacht, die die seit der Aufklärung geltenden Machtbegrenzungs- und Kontrollmechanismen ersetzen, sind nicht in Sicht. Die **Militarisierung der Polizei** schreitet auch voran durch Auslandseinsätze von Polizisten und gemeinsame CRC-Übungen (Crowd and Riot Control) von Polizeibeamten einerseits, Soldaten andererseits. Die Befugnisse der Bundeswehr zu Einsätzen im Inland wurden erweitert, das Militär wurde verfassungswidrig im Inland gegen Proteste gegen den G 8-Gipfel in Heiligendamm 2007 eingesetzt.

1.5 Europäisches und internationales Sicherheitsrecht

Weitere Einflüsse folgen aus der **Europäisierung und Internationalisierung des Polizeirechtes** z.B. durch die Gemeinsame Sicherheits- und Außenpolitik in Europa (GASP) mit dem Haager Programm zur gemeinsamen Justiz- und Innenpolitik, Kompetenzerweiterungen für EUROPOL (europäisches Polizeiamt), Ausbau des Schengener Informationssystems (SIS und SIS II), Ausbau von FRONTEX (Europäische Grenzschutzagentur zur Kontrolle der Außengrenzen), EUROJUST (Europäische Justizbehörde für Koordinierung und Informationsaustausch im Justizbereich und der Ermittlungsbehörden), dem Vertrag von Prüm (vereinfachter Datenaustausch, operative Zusammenarbeit Polizei, Strafverfolgungsbehörden, Ausländerbehörden in Europa), dem Aufbau biometrischer Datenbanken (VIS -Visainformationssystem und EURODAC mit Zugriffsmöglichkeiten für EUROPOL), der Fluggastdatenübermittlung im internationalen Flugverkehr, dem Kooperationsverbund der Anti-Terror-Spezialeinheiten (ATLAS-Gruppe) und dem geplanten Europäischen Informationsverbund für Daten der Sicherheitsbehörden und Geheimdienste.

1.6 Privatisierung der Sicherheit

Schließlich ist auch die **Einbindung Privater**, Nicht-Hoheitsträger, in Polizeiaufgaben zu erwähnen: Hilfspolizisten und private Unternehmen erhalten Zugang zu Hoheitsaufgaben und Sicherheitsinformationen der Polizei, aber auch zu sog. „Gefährderdateien“, z.B. bei Fußball-Großereignissen. Sicherheitsaufgaben werden privatisiert.

Private Unternehmen werden - etwa bei Rasterfahndung und Vorratsdatenspeicherung - für Sicherheitsaufgaben herangezogen, mit unbekannten Auswirkungen auf die Zugriffsmöglichkeiten der dadurch entstehenden Datenbestände (s. Telekomskandal).

1.7 Folgerungen

Die Überprüfung des Landespolizeirechtes muß diese Veränderungen der Sicherheitslandschaft“ einbeziehen:

Wesentliche Sicherheitsaufgaben im Bereich „Terror“ und „Organisierte Kriminalität“ werden sukzessive in die Bundeskompetenz bzw. auf die Europäische und internationale Ebene verlagert. Mit derartigen Gefahren können daher mit abnehmender Tendenz Befugnisse für die Landespolizei nicht mehr gerechtfertigt werden, die ja nur Befugnisse im eigenen Kompetenzbereich benötigt, nicht aber „auf Vorrat“ für Aufgaben, die woanders zentralisiert werden. Mit dem Ausbau der Bundes- und Europakompetenz muß daher eine „Entschlackung“ der Landespolizeibefugnisse einhergehen, denn eine Vervielfachung der Eingriffsbefugnisse ist auch für eine effiziente Polizeiarbeit nicht wünschenswert, schon wegen der damit verbundenen Unübersichtlichkeit der gesetzlichen Voraussetzungen. Der Schutz vor Terrorgefahren ist nicht mehr Sache der Landespolizei, wenn er vom Bund und der Internationalen Gemeinschaft übernommen wird.

Verschiedene Parallelbefugnisse schaffen nur Verwirrung und Fehlerquellen, wie beispielsweise die amerikanischen Sicherheitsbehörden in der Analyse der Fehler vor dem 11.09.2001 festgestellt haben.

Die auf allen Ebenen ausufernden Datenerhebungs-, Datenspeicherungs-, Datenverwendungs- und Datenaustauschmöglichkeiten lassen die beschränkende Funktion der **Zweckbindung von Daten** entfallen und schaffen ausufernde Nutzungs- und Verknüpfungsmöglichkeiten, die die **Freiheit, Würde und Selbstbestimmung** der Bürgerinnen und Bürger bedrohen. Alle Möglichkeiten der Datenerhebung, Datenspeicherung und Datenverwendung müssen vor dieser veränderten Sicherheitslandschaft neu beurteilt werden.

Mißbrauchsmöglichkeiten bei der Nutzung umfangreicher Datenbestände müssen auf allen Ebenen als realistische Gefahr mit abgewogen werden.

Nicht zuletzt sei darauf verwiesen, daß der **Nutzen des rasanten Umbaus** der „Sicherheitsarchitektur“ bislang weder erwiesen noch geprüft wurde. Bürgerrechte wurden großzügig relativiert und geopfert **ohne Evaluierung** des sicherheitstechnischen Gewinns.

Die Erfahrungen gerade im Umfeld der Proteste gegen das Gipfeltreffen in Heiligendamm 2007, aber auch schon bei Castor-Transporten und anderen Bürgerprotesten zeigen, daß die Überwachungsermächtigungen in der Praxis bisher sehr großzügig, in hohem Maße unverhältnismäßig und daher verfassungswidrig angewendet wur-

den[2]. Erwiesener Mißbrauch durch Polizeibehörden muß ebenso untersucht werden, wie der tatsächliche Nutzen der neuen Sicherheitstechnik in der Praxis für den behaupteten Zweck der Abwehr schwerer Gefahren und die Zuverlässigkeit der technischen Einrichtungen gemessen an der Einführungspropaganda[3].

2 Aktuelle Rechtsprechung des Bundesverfassungsgerichtes

Das Bundesverfassungsgericht hat in den letzten Jahren eine Vielzahl von Verfassungsbeschwerden und Normenkontrollverfahren zu Polizei- und Sicherheitsgesetzen entschieden und dabei die verfassungsrechtlichen Anforderungen an das „neue Sicherheitsrecht“ konkretisiert:

- Großer Lauschangriff, Urteil vom 03.03.2004 - 1 BvR 2138/98 und 1 BvR 1084/99
- Telefonüberwachung nach dem Außenwirtschaftsgesetz, Beschluß vom 03.03.2004 - 1 BvF 3/92
- Handy-Beschlagnahme, Beschluß vom 04.02.2005 - 2 BvR 308/04
- Daten(träger)beschlagnahme, Beschluß vom 12.04.2005 - 2 BvR 1027/02
- GPS-Überwachung, Urteil vom 12.04.2005 - 2 BvR 581/01
- Niedersächsisches Gesetz über die öffentliche Sicherheit und Ordnung, Urteil vom 27.07. 2005 (TKÜ) - 1 BvR 668/04
- TK-Verbindungsdatenspeicherung, Urteil vom 02.03.2006 - 2 BvR 2099/04
- Durchsuchung und Datenbeschlagnahme in Redaktionsräumen, Urteil vom 27.02.2007 - 1 BvR 538/06 und 2045/06 (Cicero)
- Rasterfahndung, Beschluß vom 04.04.2006 - 1 BvR 518/02
- Luftsicherheitsgesetz, Urteil vom 15.02.2006 - 1 BvR 357/05
- Mobilfunk-Überwachung/Berufsschutz, Beschluß vom 18.04.2007 - 2 BvR 2094/05
- Videoüberwachung/Kunst, Beschluß vom 23.02.2007 - 1 BvR 2368/06
- TKÜ/Berufsschutz, Beschluß vom 30.04.2007 - 2 BvR 2151/06
- akustische Wohnraumüberwachung, Beschluß vom 11.05.2007 -2 BvR 543/06
- Online-Kontenabruf, Beschluß vom 13.06.2007 - 1 BvR 1550/03 u.a.
- Online-Durchsuchung, Urteil vom 27.02.2008 - 1 BvR 370/07 u. 1 BvR 595/07
- Automatisierter Kfz-Kennzeichenabgleich in Hessen und Schleswig-Holstein, Urteil vom 11.03.2008 - 1 BvR 2074/05 und 1 BvR 1254/07

---

[2] Erhebliche Vorfeldüberwachungsmaßnahmen wurden inzwischen von den Gerichten als rechtswidrig eingestuft, so große Lauschangriffe, das Abhören von Telefonaten mit Anwälte, Postbeschlagnahme in Hamburg, Geruchsproben, aber auch Hunderte von Gewahrsamnahmen und Platzverweisen „zur Verhinderung von Straftaten mit erheblicher Bedeutung“, s. auch die Berichte des Landebeauftragten für den Datenschutz Mecklenburg-Vorpommern vom 11.06., 25.06. und 04.09.2007, www.lfd-mv.de

[3] sehr informativ hierzu die Auswertung der Videoüberwachung in Groß-Britannien: danach konnten Bilder von Überwachungskameras trotz flächendeckendem Einsatz nur bei 3% der Straftaten zur Aufklärung beitragen, vgl. The Guardian vom 06.05.2008 http://www.guardian.co.uk/uk/2007/may/06/ukcrimel/AR; s. hierzu auch Noé Leblanc, Big Brother ist kurzsichtig - der zweifelhafte Nutzen der Überwachungskameras, Le Monde Diplomatique September 2008, S. 18

- TK-Vorratsdatenspeicherung, Eilbeschluß vom 11.03.2008 - 1 BvR 256/08

In all diesen Entscheidungen betont das Bundesverfassungsgericht deutlich und mit steigender Tendenz folgende **fünf Prüfungskriterien** für die Verfassungsmäßigkeit präventivpolizeilicher Eingriffsakte und Ermächtigungsnormen:

- Gesetzgebungskompetenz, speziell im Grenzbereich „Straftatenvorsorge“ und „vorbeugender Verbrechensbekämpfung“[4]
- Normenklarheit und Bestimmtheitsgebot[5]
- Grundrechtsschutz durch Verfahren[6]
- Absolute Grenzen: Menschenwürde[7], Schutz des privaten Kernbereichs[8], Berufsschutz[9]
- Verhältnismäßigkeit, speziell bei Eingriffen in das informationelle Selbstbestimmungsrecht[10]

Neue technische Entwicklungen und automatisierte Überwachungsmaßnahmen können durch die vielfachen Datenverwendungs- und -verknüpfungsmöglichkeiten die Intensität von Eingriffen in das informationelle Selbstbestimmungsrecht erhöhen. Daher verlangt das Bundesverfassungsgericht wegen der raschen technischen Entwicklung, daß der Gesetzgeber selbst beobachtet und überprüft, ob die bestehenden verfahrensrechtlichen Vorkehrungen für einen effektiven Grundrechtsschutz (noch) ausreichen und auch, ob polizeiliche Überwachungsmaßnahmen in ihrer praktischen Anwendung für den angestrebten Erfolg - etwa: die Aufklärung organisierter Kriminalität - tauglich sind.[11] Dies bedeutet eine Pflicht des Gesetzgebers zur laufenden Evaluierung der neuen technischen Überwachungsmaßnahmen im Hinblick auf ihre Anwendung und ihren Nutzen in der polizeilichen Praxis.

2.1 Abgrenzung der Gesetzgebungskompetenz bei der Straftatenvorsorge

In der Entscheidung zur präventivpolizeilichen Telefonüberwachung in Niedersachsen[12] trifft das Bundesverfassungsgericht grundsätzliche Aussagen zur Gesetzgebungskompetenz der Länder in Abgrenzung zum Bundesgesetzgeber bei der „Straftatenvorsorge“. Dieser Begriff umfaßt sowohl die Straftatenprävention, als auch die Vorsorge für die künftige Verfolgung von Straftaten.

---

[4] U. 27.07. 2005 - 1 BvR 668/04 - zur TKÜ nach NdsSOG
[5] U. v. 3 03 2004 - 1 BvR 2378/98 - Gr. Lauschangriff; B. v. 27.07.2005 - 1 BvR 668/04 - NdsSOG; B. v. 12.03.2004 - 1 BvF 3/92 - Außenwirtschaftsgesetz; B. v. 04.04.2006 - 1 BvR 1518/02 - Rasterfahndung; B. v. 23.02.2007 - 1 BvR 2368/06- VÜ-Kunst; B. v. 13.06.2007 - 1 BvR 1550/03 - Kontenabruf; B. v. 27.02.2008 - 2 BvR 370/07 - Online-Durchsuchung; v. 11.03.2008 - 1 BvR 2074/05 - Kfz-Kennzeichenabgleich
[6] U. v. 03.03.2004 - 1 BvR 2378/98 - Gr. Lauschangriff
[7] U. v. 15.02.2006 - 1 BvR 357/05 Luftsicherheitsgesetz
[8] U. v. 03.03.2004 - 1 BvR 2378/98 - Gr. Lauschangriff;
[9] B. v. 12.04. 2005 - 2 BvR 1027/02; B. v. 30.04.2007 - 2 BvR 2151/06
[10] z.B. v. 11.03.2008 - 1 BvR 2074/05 und 1 BvR 1254/07
[11] v. 12.04.2005 - 2 BvR 581/01 - GPS;
[12] U. v. 27.02.2005 - 1 BvR 668/04

Gegenstand der Prüfung des Bundesverfassungsgerichtes vom 27.07.2005 war die Ermächtigung zu Eingriffen in das Fernmeldegeheimnis nach § 33 a NdsSOG bei Personen,

> „*bei denen Tatsachen die Annahme rechtfertigen, dass sie Straftaten von erheblicher Bedeutung begehen werden".*

Das Bundesverfassungsgericht untersucht zunächst den Zweck der Maßnahme zwischen Gefahrenabwehr, Gefahrverhütung, Straftatenverhütung, Straftatenvorsorge oder Vorsorge für die künftige Strafverfolgung. Nur für (rein) präventive (Gefahren verhütende) Zwecke besteht die ausschließliche Gesetzgebungskompetenz des Landes, während im Bereich der Strafverfolgung und des gerichtlichen Verfahrens der Bund nach Art. 74 Abs. 1 GG die konkurrierende Gesetzgebung hat, die er mit der Strafprozeßordnung ausgeschöpft hat, und zwar umfangreich auch im Vorfeld der Straftat, z.B. in §§ 100 ff StPO.

Das Bundesverfassungsgericht ordnet dann die Datenerhebung jenseits eines konkreten strafrechtlichen Anfangsverdachtes, die nicht die *präventive Datenerhebung zur Verhütung von Straftaten*, sondern die *Beweisbeschaffung zur Verwendung in künftigen Strafverfahren* bezwecken, der **Verfolgungsvorsorge** und daher dem *gerichtlichen Verfahren* zu mit der Folge, daß die Gesetzgebungskompetenz nach Art. 74 Abs. 1 Nr. 1 GG dem Bund zusteht. Das Bundesverfassungsgericht fordert hier eine genaue Abgrenzung, damit die vom Bundesgesetzgeber im Rahmen der konkurrierenden Gesetzgebung beschlossenen Eingriffsschranken zu demselben Ziel - der Sicherung späterer Strafverfolgung - nicht durch Parallelregelungen auf Landesebene unterlaufen werden können. Widersprüchliche Parallelregelungen oder Überschneidungen unterschiedlicher Normen müßten vermieden werden. Daher sieht das Bundesverfassungsgericht die Gesetzgebungskompetenz „zur Straftatenvorsorge" beim Bund und die Vorschriften der Strafprozeßordnung zur Überwachung der Telekommunikation als abschließend an.

Diese Grundsätze sind auf alle anderen Befugnisse zur Straftatenvorsorge entsprechend anwendbar. Strafprozessuale Grenzen und Verfahrensgarantien dürfen nicht präventivpolizeilich unterlaufen werden.[13] Soweit die Strafprozeßordnung Regelungen für die Straftaten(verfolgungs)vorsorge enthält, fehlt dem Landesgesetzgeber die Gesetzgebungskompetenz, weil der Bundesgesetzgeber sie *zur Strafverfolgung oder zur Verfolgung und Beweissicherung für künftige Straftaten* ausgeübt hat.[14]

2.2 Bestimmtheitsgebot, Normenklarheit

Ebenfalls in der Entscheidung zur Telekommunikationsüberwachung in Niedersachsen[15] und in vielen weiteren Entscheidungen[16] betont das Bundesverfassungsgericht

---

[13] Denninger in Lisken/Denninger, Handbuch des Polizeirechtes Kap E Anm. 174 und 192 ff.

[14] Gerade im Bereich der Datenverarbeitung ist hier im einzelnen ist hier noch vieles streitig, weil es Überschneidungen und sog. „doppelfunktionale Maßnahmen" gibt. Die Instanzgerichte nehmen z.B. im Bereich der erkennungsdienstlichen Behandlung nach § 81 b 1. Alt. StPO oder bei der Datenspeicherung von strafprozessual erhobenen Daten durch die Polizei für präventive Zwecke nach § 484 Abs. 4 StPO andere Abgrenzungen im Bereich der „Straftatenvorsorge" und „Verfolgungsvorsorge" vor, als das BVerfG, vgl. z.B. OVG Schleswig, B. v. 15.03.2007 - 4 MB 5/07 (juris), VGH München, B. v. 24.07.2008 - 10 C 08.1780 (juris)

[15] B. v. 27.07.2005 - 1 BvR 668/04

[16] z.B. B. v. 03.03.2004 - 1 BvF 3/92 - Außenwirtschaftsgesetz; B. v. 04.04.2006 - 1 BvR 1518/02 - Rasterfahndung; B. v. 23.02.2007 - 1 BvR 2368/06- VÜ-Kunst; B. v. 13.06.2007 - 1 BvR 1550/03 -

die Anforderungen an die **Normenbestimmtheit und Normenklarheit** im polizeilichen Eingriffsrecht.

Die Grundlage des Bestimmheitsgebotes wird im jeweils betroffenen Freiheitsgrundrecht selbst angesiedelt: Betroffene Bürger sollen sich auf mögliche belastende Maßnahmen einstellen können, die Verwaltung soll steuernde und begrenzende Handlungsmaßstäbe im Gesetz selbst finden, Gerichte eine klare Kontrollgrundlage vorfinden. Das Bundesverfassungsgericht verlangt, dass **Anlaß, der Zweck und die Grenzen** des Eingriffs in der Ermächtigung **bereichsspezifisch, präzise und normenklar** festgelegt werden. Die Entscheidung über die Grenzen der Freiheit des Bürgers **darf nicht einseitig in das Ermessen der Verwaltung gestellt** sein.

Im Vorfeld der Gefahrenabwehr oder der Strafverfolgung, also im Bereich der Verhütung künftiger Straftaten oder Gefahren, fehlt es sowohl an einer konkreten Gefahrenlage als auch an einem konkreten Tatverdacht als begrenzendem Eingriffskriterium. Dies stellt besondere Anforderungen an die Bestimmtheit der Eingriffsbefugnis, denn im Vorfeld einer konkreten Tat oder Gefahr beruhen Sachverhaltsfeststellung und polizeiliche Prognose auf „vorgreiflichen Einschätzungen über das weitere Geschehen“ sowie auf Tatsachenzusammenhängen, deren weiterer Verlauf verschiedene Deutungsalternativen zuläßt. Damit ist die Vorfeldermittlung von einer „*hohen Ambivalenz der potentiellen Bedeutung einzelner Verhaltensumstände geprägt“* und damit mit einem besonders hohen Risiko der Fehlprognose behaftet. Das Gesetz selbst muß bei Vorfeldeingriffen daher klare eingriffsbeschränkende Maßstäbe enthalten. Auch das Erfordernis einer richterlichen Anordnung gleicht Bestimmheitsdefizite nicht aus, denn auch der Richter muß Anhaltspunkte für die Kontrolle im Gesetz selbst vorfinden.

Bestimmtheitsprobleme und darüber hinaus Probleme der Verhältnismäßigkeit ergeben sich ähnlich für Eingriffe mit großer Streubreite[17], also solche, die sowohl potentielle Straftäter oder „Gefährder“, als auch Dritte wie Angehörige und Kontaktpersonen und Menschen, die selbst keinen Überwachungsanlaß gegeben haben, betreffen. Je ungenauer die tatsächlichen Voraussetzungen des Eingriffs im Gesetz geregelt sind, umso größer ist das Risiko unangemessener Maßnahmen im Einzelfall. Im Einzelfall kommt es immer auf die Abwägung des geschützten Rechtsgutes, der Intensität der ihm drohenden Gefahr und der Intensität des Eingriffs an. Das Abwägungsgebot kann seine Begrenzungsfunktion nur entfalten, wenn das Gewicht des geschützten Rechtsgutes, die Intensität und die Wahrscheinlichkeit der ihm drohenden Gefahr sowie die tatsächlichen Anforderungen für die Annahme von Gefährdungsumständen im Gesetz selbst bestimmt sind. Bei geringem Gewicht des gefährdeten Rechtsgutes etwa steigen die Anforderungen an die Prognosesicherheit hinsichtlich der drohenden Gefahr und der Wahrscheinlichkeit eines Schadenseintrittes.[18]

In der Entscheidung zum Kfz-Kennzeichenabgleich in Hessen und Schleswig-Holstein hat das Bundesverfassungsgericht die Anforderungen an Normenbestimmtheit und Normenklarheit bei polizeilichen Eingriffsakten erneut betont[19]. Danach muß der Gesetzgeber selbst die Eingriffsvoraussetzungen, den Zweck der Maßnahme

---

Kontenabruf; B. v. 27.02.2008 - 2 BvR 370/07 - Online-Durchsuchung; v. 11.03.2008 - 1 BvR 2074/05 - Kfz-Kennzeichenabgleich

[17] B. v. 27.07.2005 - 1 BvR 668/04 Nds. SOG; B. v. 04.04.2006 - 1 BvR 1518/02 Rasterfahndung

[18] ebd,

[19] BVerfG v. 11. März 2008 -1 BvR 2074/05; U. v. 03.04.2005 - 1 BvR 2378/98 Gr. Lauschangriff

und beim Datenabgleich die Datenbestände bestimmen, mit denen abgeglichen werden soll.

Auch technische Eingriffsinstrumente muß der Gesetzgeber genau bezeichnen und dadurch sicherstellen, daß der Adressat den Inhalt der Norm jeweils erkennen kann[20]. Zwar sei die Einbeziehung kriminaltechnischer Neuerungen nicht ausgeschlossen, jedoch muß wegen des schnellen und für den Grundrechtsschutz riskanten informationstechnischen Wandels der Gesetzgeber die technischen Entwicklungen aufmerksam beobachten. Bei Fehlentwicklungen durch die konkrete Ausfüllung offener Gesetzesbegriffe durch Behörden und die Gerichte muß der Gesetzgeber notfalls durch ergänzende Rechtssetzung korrigierend eingreifen.[21] Für die Wohnraumüberwachung nach § 100 c StPO (n.F.) hat das Bundesverfassungsgericht dann angenommen, die Eingriffsbefugnis sei hinreichend bestimmt durch die systematische Abgrenzung von optischer Überwachungstechnik einerseits, akustischer Überwachungstechnik andererseits. Dies gelte allerdings nicht,

> *„ wenn neue Technik zu einem Observationsinstrument besonderer Art und spezifischer Tiefe werden könnte, dessen Einsatz von Verfassungs wegen nur unter restriktiveren Voraussetzungen gestattet werden darf.“*[22]

In der Entscheidung zur Telefonüberwachung nach dem Außenwirtschaftsgesetzstellt das Bundesverfassungsgericht weitere Anforderungen an Bestimmtheit und Normenklarheit:

> *„Erreicht der Gesetzgeber die Festlegung des Normeninhalts aber - wie hier - nur mit Hilfe zum Teil langer, über mehrere Ebenen gestaffelter, unterschiedlich variabler Verweisungsketten, die bei gleichzeitiger Verzweigung in die Breite den Charakter von Kaskaden annehmen, leidet die praktische Erkennbarkeit der maßgebenden Rechtsgrundlage. Der Prüfvorgang wird dadurch fehleranfällig. Gerade in Eilfällen besteht eine gesteigerte Gefahr von Fehlentscheidungen der Verwaltung und der eingeschalteten Gerichte…. Auch für die Bürger als Normadressaten ist bei Regelungen mit tiefgestaffelten Verweisungen schwer erkennbar, worauf mögliche gestützt werden können.“*[23]

2.3 Grundrechtsschutz durch Verfahren

Zum Grundrechtsschutz bei **besonders intensiven, heimlichen Grundrechtseingriffen** verlangt das Bundesverfassungsgericht zum Ausgleich Verfahrenssicherungen. Eine besondere Eingriffsintensität folgt aus heimlichen Überwachungen, besonders persönlichkeitsrelevanten Überwachungen (mit der Gefahr von „Rundumüberwachung“, Bewegungsprofilen oder Persönlichkeitsbildern), aus „additiven Eingriffen“ mit Datenverknüpfungsmöglichkeiten aus verschiedenen Überwachungsmaßnahmen und bei Eingriffen mit hoher Streubreite für Drittbetroffene, die selbst keinen Ermittlungsanlaß gegeben haben, außerdem bei Nähe zum Kernbereich oder Schutz besonderer Vertrauensverhältnisse (s. u. 2.4).

---

[20] ebd. unter Hinweis auf BVerfGE 87, 287,317 f.
[21] ebd. unter Hinweis auf BVerfGE 90, 145,191
[22] BVerfG, U. v. 12.04.2005 - 2 BvR 581/01
[23] v. 03.03.2004 - 2 BvF 3/92 - Außenwirtschaft

Zum Grundrechtsschutz durch Verfahren[24] gehören

- **Richtervorbehalt**
- **Benachrichtigungspflichten** nach Abschluß heimlicher Maßnahmen, auch für Drittbetroffene, zur Gewährleistung **effektiven Rechtsschutzes**
- **Verwertungsverbote** für rechts- oder grundrechtswidrig erlangte Informationen (etwa bei Verstoß gegen den Kernbereichsschutz)
- **Löschungspflichten** für rechtswidrig erlangte oder nicht mehr benötigte Daten
- **Kennzeichnungspflichten** für Daten, die aus besonderen Überwachungsmaßnahmen stammen
- **Protokollierungspflichten** für die Übermittlung von Daten aus besonderen Überwachungen
- **Kontrollmaßnahmen** des Gesetzgebers (Parlamentarische Kontrollgremien, befristete Einführung von Maßnahmen, Evaluierung)

Dieser Katalog ist nicht abschließend, sondern ist - je nach Art der neuartigen Überwachungsmaßnahmen - fortzuschreiben mit der technischen Entwicklung.

In der Entscheidung zur GPS-Überwachung nach § 100 c StPO (Einsatz technischer Mittel zur Ermittlung des Aufenthaltsortes oder zur Sachverhaltserforschung) im strafrechtlichen Ermittlungsverfahren hat das Bundesverfassungsgericht ausgeführt[25]:

- Beim Einsatz moderner, insbesondere dem Betroffenen verborgener, Ermittlungsmethoden müssen die Strafverfolgungsbehörden mit Rücksicht auf das dem „additiven“ Grundrechtseingriff innewohnende Gefährdungspotential besondere Anforderungen an das Verfahren beachten.
- Wegen des schnellen und für den Grundrechtsschutz riskanten informationstechnischen Wandels muß der Gesetzgeber die technischen Entwicklungen aufmerksam beobachten und notfalls durch ergänzende Rechtssetzung korrigierend eingreifen. Dies betrifft auch die Frage, ob die bestehenden verfahrensrechtlichen Vorkehrungen angesichts zukünftiger Entwicklungen geeignet sind, den Grundrechtsschutz effektiv zu sichern und unkoordinierte Ermittlungsmaßnahmen verschiedener Behörden verläßlich zu verhindern.

Grundrechtsschutz durch Verfahrenssicherungen ergibt sich zum einen unmittelbar aus den verfassungsrechtlichen **Richtervorbehalten** für Eingriffe in besonders hochrangige Grundrechte (Art. 10, 13, 104 GG). Das Bundesverfassungsgericht sieht auch in einfachgesetzlich normierten Richtervorbehalten für besonders intensive Grundrechtseingriffe eine Grundrechtssicherung, vor allem für heimliche Eingriffe, von denen der Betroffene - jedenfalls während des Eingriffs - nichts erfährt[26]. Art. 19

[24] BVerfG, u . v. 03.03.2004 - 1 BvR 2378/98 - Gr. Lauschangriff
[25] vom 12.04.2005 - 2 BvR 581/01
[26] so BVerfG, U. v. 27.02.2008 - 1 BvR 370/07 - Online-Durchsuchung

Abs. 4 GG in Verbindung mit dem Rechtsstaatsprinzip verlangt bei jedem Grundrechtseingriff die Möglichkeit, effektiven Rechtsschutz zu erlangen. Bei heimlichen Maßnahmen muß dies durch den Richtervorbehalt als „Justizersatz“ kompensiert und durch anschließende Benachrichtigung ermöglicht werden. Behördenleitervorbehalte stehen dem Richtervorbehalt nicht gleich, da sie keine justizförmige Prüfung der Eingriffsvoraussetzungen ermöglichen, sondern nur eine Zweckmäßigkeitskontrolle und „Leichtfertigkeitsschranke“ darstellen.

Das Gebot von Verfahrenssicherungen bei intensiven Grundrechtseingriffen - insbesondere bei heimlichen Überwachungsmaßnahmen, bei Vorfeldverlagerung im Zusammenhang mit schwerwiegenden Gefahren für hochrangige Rechtsgüter oder bei erheblicher Streubreite von Eingriffen - folgt außerdem aus dem **Verhältnismäßigkeitsprinzip**. Hier soll etwa ein Richtervorbehalt eine zusätzliche **Mißbrauchssicherung** und Verhältnismäßigkeitskontrolle im Einzelfall bewirken und die Heimlichkeit des Eingriffs ausgleichen.

Eine Eingriffsbefugnis für heimliche Maßnahmen muß zudem eine Pflicht zur wenigstens nachträglichen **Benachrichtigung** enthalten, sobald der Maßnahmezweck nicht mehr gefährdet ist, um wenigstens nachträglich effektiven Rechtsschutz (Art. 19 Abs. 4 GG) zu ermöglichen.

Zu benachrichtigen sind der Betroffene, gegen den sich die Maßnahme richtet, Inhaber und Bewohner einer überwachten Wohnung und Drittbetroffene[27].

Auch für den Umgang mit den besonders sensiblen Daten aus heimlichen Überwachungsmaßnahmen verlangt das Bundesverfassungsgericht in der Entscheidung zum Großen Lauschangriff Schutzvorkehrungen bereits des Gesetzgebers selbst in der Ermächtigungsnorm.[28]

Ebenfalls zum Verfahrensschutz gehört das Postulat, erlangte, aber nicht mehr benötigte Daten grundsätzlich zu vernichten, aber dabei den effektiven Rechtsschutz nicht zu behindern. **Vernichtungspflicht** und Rechtsschutzgarantie müssen so abgestimmt werden, daß Rechtsschutz nicht vereitelt wird, etwa durch Sperrung statt endgültiger Löschung der Daten bis zum Abschluß des Rechtsschutzverfahrens.

Zudem verlangt das Bundesverfassungsgericht, daß Daten, die aus besonderen Überwachungsmaßnahmen stammen, besonders **gekennzeichnet** werden[29], denn jede Weitergabe der Daten und ihre Auswertung in einem anderen Zusammenhang erhöht die Intensität des Grundrechtseingriffs. Es muß durch die gesetzliche Regelung sichergestellt werden, daß der Übermittlungszweck mit dem ursprünglichen Erhebungszweck vereinbar ist.[30] Jede Übermittlung muß **protokolliert** werden[31].

Für das strafprozessuale Ermittlungsverfahren hat das Bundesverfassungsgericht in in der Entscheidung zur GPS-Überwachung im Strafverfahren seinerzeit (vor 3 Jahren) ausreichende „Sicherung durch Verfahren“ gegen eine **unzulässige „Rundumüberwachung**“ darin gesehen, daß

---

[27] BVerfG, B. v. 03.03.2004 - 1 BvR 2378/98 - Gr. Lauschangriff
[28] ebd.
[29] so schon B. v. 03.03.2004 - 1 BvF 3/92 - Außenwirtschaftsgesetz
[30] ebd.
[31] ebd.

- dort immer die Staatsanwaltschaft informiert sein muß
- eine vollständige Aktendokumentation erforderlich ist
- durch bundesweite Aktenregister der StA sichergestellt ist, daß nicht durch Ermittlungen verschiedener Behörden zufällig eine „Rundumüberwachung“ erfolgt durch das Gefährdungspotential „additiver Grundrechtseingriffe“
- wegen der durch § 492 StPO ermöglichten Abstimmung der Sicherheitsbehörden genug Sicherung der Interessen der Betroffenen vorlägen,

aber ebenfalls ausgeführt:

> *„Der Gesetzgeber wird darüber hinaus zu beobachten haben, ob die bestehenden verfahrensrechtlichen Vorkehrungen auch angesichts zukünftiger Entwicklungen geeignet sind, den Grundrechtsschutz effektiv zu sichern. Es dürfte zu erwägen sein, ob durch ergänzende Regelung der praktischen Ermittlungstätigkeit - etwa in den Richtlinien für das Strafverfahren und das Bußgeldverfahren - unkoordinierte Ermittlungsmaßnahmen verschiedener Behörden verlässlich verhindert werden können.“*

2.4 Absolute Grenzen: Menschenwürde, Kernbereich privater Lebensgestaltung, Berufsschutz, keine „Rundumüberwachung“

Eine „Rundumüberwachung“ mit der Erstellung von „Persönlichkeitsprofilen“ ist verfassungswidrig, weil sie gegen die Menschenwürde (Art. 1 GG) verstößt. Der Mensch darf nicht zum bloßen Objekt staatlichen Handelns werden, der personale Achtungsanspruch verbietet eine Totalerfassung. Ein Kernbereich von Privatheit ist unantastbar.

2.4.1 Kernbereich privater Lebensgestaltung

Das Bundesverfassungsgericht verlangt die **Anerkennung eines absolut geschützten Kernbereichs privater Lebensgestaltung** als Teil der Unantastbarkeit der Menschenwürde bei allen, vor allem auch heimlichen, staatlichen Beobachtungen[32]. Bereits eine gesetzliche Ermächtigung zur akustischen Wohnraumüberwachung oder anderen heimlichen Beobachtungen muß entsprechende Sicherungen enthalten. Insbesondere muß dem Menschen in seinen Wohnräumen *„das Recht, in Ruhe gelassen zu werden*“ garantiert sein[33]. Ebenso benötigt die *„vertrauliche Kommunikation… ein räumliches Substrat“* in der Privatwohnung als *„letztes Refugium der Menschenwürde“*[34].

Entsprechende gesetzliche Eingriffsbefugnisse müssen unter Beachtung der Normenklarheit und der Verhältnismäßigkeit von Eingriff zu Anlaß und Zweck der Maßnahme zusätzlich sicherstellen, daß

---

[32] U. v. 03.03.2004 - 1 BvR 2378/98 u.a. - Großer Lauschangriff
[33] ebd.
[34] ebd.

- Überwachung von vornherein unterbleibt, wenn Anhaltspunkte bestehen, daß der Kernbereich privater Lebensgestaltung tangiert wird
- bei unerwarteter Erhebung derart absolut geschützter Information die Überwachung abgebrochen und die Aufzeichnungen gelöscht werden
- ein absolutes Verwertungsverbot normiert wird.[35]

Die staatliche Überwachung in Privaträumen darf sich auch nicht auf die Kommunikation mit Personen erstrecken, zu denen der Betroffene in einem **besonderen Vertrauensverhältnis** steht, wie etwa zu Familienangehörigen und sonstigen engen Vertrauten. Es spricht eine Vermutung dafür, daß dann ein absolut geschütztes Gespräch vorliegt. Diese kann nur entkräftet werden, wenn bereits *vor* der Überwachungsmaßnahme *tatsächliche Anhaltspunkte* zumindest in typisierender Weise vorliegen, daß das Gespräch nicht den Kernbereich der höchstpersönlichen Angelegenheiten betrifft. Bei der Prognose ergeben sich Indikatoren aus der Art der Räumlichkeiten (Geschäftsräume als öffentlichere, Privaträume als persönliche Sphäre), wobei der „Rückzugsbereich" den höchsten Schutz genießt. Innerhalb der Privaträume ist allerdings keine Unterscheidung vorzunehmen. Besonderer Schutz ist auch geboten bei Anwesenheit von Personen des engsten, höchstpersönlichen Vertrauens wie in Ehe, Familie, Intimbereich.

Entsprechenden Schutz genießen Gespräche mit **Berufsgeheimnisträgern** wie Seelsorgern, Rechtsanwälten und Ärzten (nicht aber Medienvertretern und Parlamentsabgeordneten), und zwar als Teil des privaten Kernbereichs.

2.4.2 Gesetzliche Vorkehrungen zum Kernbereichsschutz

Sollte im Rahmen einer Wohnraumüberwachung eine Situation eintreten, die dem unantastbaren Kernbereich privater Lebensgestaltung zuzurechnen ist, muß die Überwachung *abgebrochen* werden. Dennoch erfolgte Aufzeichnungen sind zu *vernichten*. Die Weitergabe und Verwertung der gewonnenen Informationen sind untersagt. Art. 13 Abs. 3 GG ist dahingehend auszulegen, daß bei entsprechenden Aufzeichnungen *Beweisverwertungsverbote* bestehen müssen.[36] Die gesetzlichen Vorschriften müssen selbst hinreichende Vorkehrungen dafür treffen, daß Eingriffe in den absolut geschützten Kernbereich privater Lebensgestaltung unterbleiben und damit die Menschenwürde gewahrt wird. Wird dieses Verbot verletzt oder greift eine Maßnahme *unerwartet* in den absolut geschützten Kernbereich privater Lebensgestaltung ein, muß sie abgebrochen werden, und es muß durch Löschungspflichten und Verwertungsverbote vorgesorgt sein, daß die Folgen beseitigt werden.

In der Entscheidung vom 11.05.2007 zur Neuregelung des Lauschangriffs in § 100 c StPO hat das Bundesverfassungsgericht auch eine automatische Aufzeichnung für zulässig gehalten, soweit keine Gefahr der Erfassung kernbereichsrelevanter Gespräche besteht.[37]

Die Beachtung der von Verfassungs wegen bestehenden Beweisverwertungsverbote bedarf außerdem einer ergänzenden *verfahrensrechtlichen Sicherung* durch eine

---

[35] so zuletzt BVerfG, u. v. 27.02.2008 - 1 BvR 370/07 - Online-Durchsuchung

[36] zur verfassungsrechtlichen Verankerung solcher Gebote vgl. BVerfGE 44, 353,383 f.; vgl. auch BVerfGE 34, 238, 245 ff.

[37] B. v. 11.05.2007 - 2 BvR 543/06

eindeutige Regelung, wer diese Entscheidung zu beantragen hat und daß eine Verpflichtung zur Einschaltung des Gerichts besteht[38].

2.4.3 keine Rundumüberwachung

Eine „Rundumüberwachung“ ist von Verfassungs wegen stets unzulässig [39], wenn damit ein umfassendes *Persönlichkeitsprofil* eines Beteiligten erstellt werden könnte. Das ist durch allgemeine verfahrensrechtliche Sicherungen auch ohne spezifische gesetzliche Regelung grundsätzlich ausgeschlossen[40]. Eine solche Rundumüberwachung ist mit der Menschenwürde nicht zu vereinbaren (s. dazu auch unten 2. 6. Recht auf informationelle Selbstbestimmung).

2.4.4 Menschenwürde und Recht auf Leben

In der Entscheidung zum Luftsicherheitsgesetz [41] betont das Bundesverfassungsgericht die **Bedeutung des Rechts auf Leben (Art. 21 Abs. 2 S. 1 GG) in Verbindung mit der Menschenwürdegarantie (Art. 1 Abs. 1 GG)** und verbietet, tatunbeteiligte Menschen zum Objekt einer Rettungsaktion zum Schutze anderer zu machen. Dies gilt insbesondere auch dann, wenn die Betroffenen ohnehin in einer tödlichen Gefahr schweben, denn niemand ist verpflichtet, sein Leben für andere oder das Gemeinwohl zu opfern.

2.4.5 Berufsschutz

Die Überwachung der Kommunikation zwischen Strafverteidiger und Beschuldigten verstößt gegen die Rechtgarantien auf einen unüberwachten Verkehr mit dem Verteidiger (§ 148 StPO), Diese Garantie hat Verfassungsrang, weil sie zur Wahrung der Menschenwürde verhindert, daß der Beschuldigte zum bloßen Objekt im Strafverfahren wird[42].

Auch unterliegen berufsbezogene Gespräche mit Rechtsanwälten besonderen verfassungsrechtlichen Schutz: Die Berufsausübungsfreiheit (Art. 12 Abs. 1 GG) gewährleistet dem Rechtsanwalt eine von staatlicher Kontrolle und Bevormundung freie Berufsausübung und stellt das Vertrauensverhältnis zwischen Rechtsanwalt und Mandant unter besonderen Schutz; die anwaltliche Tätigkeit liegt auch im Interesse der Allgemeinheit an einer wirksamen und geordneten Rechtspflege.[43]

2.5 Verhältnismäßigkeit

---

[38] zu den vorstehenden Ausführungen im einzelnen s. BVerfG, B. v. 03.03.2004 - 1 BvR 2378/98 u.a.
[39] vgl. BVerfGE 65, 1 , 43; 109, 279, 323
[40] BVerfG, B. v. 12.04.2002 - 2 BvR 581/01
[41] U. v. 15.02.2006 - 1 BvR 357/05
[42] BVerfG., B. v. 03.03.2004, 1 BvF 3/92 - AußenwirtschaftsG
[43] BVerfG ,B. v. 12.04.2005 - 2 bvR 1027/02; B. v. 30.04.2007 - 2 BvR 2151/06

Tragendes Prinzip des Grundrechtsschutzes ist das Prinzip der Verhältnismäßigkeit:

> *„Der Grundsatz der Verhältnismäßigkeit verlangt, dass die jeweilige Maßnahme einen verfassungsrechtlich legitimen Zweck verfolgt und zu dessen Erreichung geeignet, erforderlich und verhältnismäßig im engeren Sinne ist. Der Eingriff darf den Betroffenen nicht übermäßig belasten, muss diesem also zumutbar sein.“*[44]

Das Verhältnismäßigkeitsprinzip ist sowohl vom Gesetzgeber selbst in der generellen Eingriffsbefugnis als auch vom Rechtsanwender im Einzelfall zu beachten. Je intensiver der Eingriff, desto höher die Anforderungen an die Eingriffsvoraussetzungen (tatsächliche Grundlagen des Verdachtes, Schwere der Gefahr, keine milderen Mittel verfügbar).

Bei der Prüfung der Verhältnismäßigkeit der Erfassung von Kommunikationsdaten ist ihre besondere Schutzwürdigkeit zu beachten, da solche Daten Rückschlüsse auf Kommunikations- und Bewegungsverhalten sowie auf die Art und Intensität von Beziehungen zulassen, die bis zu der Erstellung eines Persönlichkeitsprofils heranreichen können. Das Gewicht des Eingriffs wird gesteigert, wenn auch in Kommunikationsdaten von Nicht-Beschuldigten eingegriffen wird. Auf der anderen Seite müssen die Strafverfolgungsbehörden damit Schritt halten, dass das Kommunikaitonsverhalten sich in den elektronischen Nachrichtenverkehr mit digitaler Speicherung verlagert.

Im Hinblick auf die Eingriffsintensität differenziert das Bundesverfassungsgericht nach der **Heimlichkeit der Maßnahme** und sieht einen geringeren Eingriff bei offenen Ermittlungsmaßnahmen. Im entschiedenen Fall war bei geringem Tatverdacht, einer erheblichen beruflichen Stigmatisierung, geringen Erfolgserwartungen an die Beschlagnahme und mäßigem öffentlichen Interesse die Maßnahme im Einzelfall unverhältnismäßig[45].

Zu beachten ist, daß die Vorverlagerung von Eingriffen in das Vorfeld des Verdachts oder der Gefahr wegen der „Streubreite“ unter Einbeziehung Unbeteiligter die Eingriffsintensität von Maßnahmen erhöht, wegen der Verhältnismäßigkeit Eingriffe also auch an gesteigerte Gefahren anknüpfen müssen. Die anlaßlose „Jedermann-Kontrolle“ scheitert daher schon am Prinzip der Verhältnismäßigkeit.[46] Die Vorverlagerung in das Vorfeld der Gefahr „zur Verdachtsgewinnung“ ist auch deswegen ein intensiverer Eingriff in die Grundrechtssphäre, weil mit der Vorverlagerung erhebliche Prognoseunsicherheiten verbunden sind[47]

Ist ungewiß, ob polizeiliche Überwachungsmaßnahmen für den angestrebten Erfolg - etwa: Aufklärung organisierter Kriminalität - **tauglich** sind, verlangt das Gebot der Verhältnismäßigkeit , die Entwicklung zu beobachten und **fortlaufend zu prüfen**, ob das Ermittlungsinstrument tatsächlich geeignet ist, auch das mit ihm verfolgte spezielle Ziel in hinreichendem Maße zu erreichen[48].

Ferner verlangt das Bundesverfassungsgericht **bei besonders schweren Eingriffen** in die Grundrechtssphäre einen **besonders schweren Anlaß** und differenziert dabei

---

[44] BVerfG in st. Rspr, so in B. v. 02.03.2006 - 2 BvR 2099/04 -TK-Verbindungsdaten
[45] ebd.
[46] s. hierzu LVerfG Mecklenburg-Vorpommern vom 21.10.1999, LVerfG 2/98 = NJ 1999, 645; BVerfG, B. v. 14.07.1999 - 1 BvR 226/94 zur Überwachung von Auslandsferngesprächen durch den BND
[47] BVerfG, u. v. 27.07.2005 - 1 BvR 668/04 NdsSOG
[48] so BVerfG, B. v. 03.03.2004 - 1BvR 2378/98 - Gr. Lauschangriff, unter Hinweis auf BVerfGE 33, 171 189 f.; 37, 104, 118; 88, 203,231 zur Überprüfung gesetzlicher Regelungen

den verfassungsrechtlichen *Begriff der „besonders schweren Straftat“* von dem strafprozessualen Begriff einer „Straftat von erheblicher Bedeutung“, die nicht gleichgesetzt werden dürfen.

Eine „Straftat von erheblicher Bedeutung“ muß mindestens der *mittleren* Kriminalität zuzurechnen sein, den Rechtsfrieden empfindlich stören und geeignet sein, das Gefühl der Rechtssicherheit der Bevölkerung erheblich zu beeinträchtigen[49].

Die von Art. 13 Abs. 3 GG vorausgesetzten „besonders schweren Straftaten“ müssen den *mittleren Kriminalitätsbereich deutlich übersteigen*. Die besondere Schwere der Anlaßtat muß sich im Einzelfall aus den *konkreten Folgen für betroffene Rechtsgüter* ergeben und nicht allgemein aus einer generellen Strafandrohung für eine Katalogstraftat. Eine besondere Schwere der Straftat setzt eine höhere Schwere als eine Höchststrafe von 5 Jahren im Strafrahmen voraus[50] Auch die Anforderungen an den Tatverdacht müssen bei schweren Grundrechtseingriffen gesteigert sein. Es müssen *konkrete und in gewissem Umfang verdichtete* Umstände als Tatsachenbasis für den Verdacht vorhanden sein, das ist mehr als ein Anfangsverdacht, muß aber kein „dringender Tatverdacht“ sein[51]. Vage Anhaltspunkte oder bloße Vermutungen rechtfertigen keine schweren Eingriffe[52]

Insgesamt verlangt das Bundesverfassungsgericht eine sorgfältige Abwägung von

- Eingriffsanlaß
- Zweck der Maßnahme
- betroffenen geschädigten oder gefährdeten Rechtsgüter generell (in der Eingriffsnorm) und im Einzelfall
- Maß des Tatverdachtes bzw. Schwere der Gefahr und Wahrscheinlichkeit des Schadenseintritts, Maß der drohenden Schäden
- Rang des betroffenen Grundrechtes, in das eingegriffen wird
- Schwere des Grundrechtseingriffs im Einzelfall

Den Ausgleich der widerstreitenden Interessen muß der Gesetzgeber generell *bereits in der gesetzlichen Regelung* und die Gerichte im Einzelfall in der Gesetzesanwendung gewährleisten. Darüber hinaus muß der Gesetzgeber auch die Wirksamkeit verfahrensmäßiger Kontrollen - etwa: des Richtervorbehaltes - sicherstellen. Dies gilt insbesondere bei heimlichen Ermittlungsmaßnahmen.

Kann gegen einen Eingriff - etwa wegen seiner heimlichen Durchführung und fehlender Benachrichtigung - nicht in angemessener Zeit **Rechtsschutz** begehrt und können seine Folgen dadurch nicht zügig beseitigt werden, erhöht dies zusätzlich die Schwere der Grundrechtsbeeinträchtigung...“[53]

2.6 Recht auf informationelle Selbstbestimmung und Integrität informationstechnischer Systeme

[49] so schon BVerfGE 103, 21, 34; 107, 299, 322

[50] vgl. BVerfG, U. v. 03.03. 2004 - 2 BvR 2378/98 - Gr. Lauschangriff

[51] vgl. BVerfGE 100, 313, 395; BVerfG v. 03.03.2004 - 2 BvR 2378/98

[52] so für Telefonüberwachung BVerfG B. v.. 30.04.2007 - 2 BvR 2151/06 und B. v. 04.07.2006 - 2 BvR 950/06

[53] BVerfG, B. v. 27.07.2005 - 1 BvR 668/05 - NdsSOG

Die vorstehenden Prinzipien unterliegen für das Grundrecht auf informationelle Besonderheiten. Moderne technische Überwachungsmaßnahmen sind gekennzeichnet durch verdachtsunabhängige Eingriffe mit hoher Streubreite einerseits und fast unbegrenzte technische Möglichkeiten zur Datenverwendung mit der Gefahr der Erstellung von **Persönlichkeits- und Bewegungsprofilen.**

Immer wieder betont das Bundesverfassungsgericht, daß sich die Intensität des Eingriffs erhöht und daher eine gesteigerte Verhältnismäßigkeitsprüfung erforderlich ist

- wenn von der Überwachung Betroffene selbst keinen **Anlaß zu der Maßnahme** gegeben haben
- bei verdachtslosen Eingriffen mit großer Streubreite[54].
- bei heimlichen Datenerhebungen
- bei automatischer Datenverarbeitung wegen der gesteigerten Gefährdung durch Verknüpfungsmöglichkeiten

Gesetzliche Regelungen, die in das informationelle Selbstbestimmungsrecht eingreifen, müssen Anlaß, Zweck und Grenzen präzise festlegen. Dazu gehört auch die Angabe des Verwendungszwecks der erhobenen Daten und bei Datenabruf die Bestimmung der Zugriffsberechtigten. Die jeweils geschützten Gemeinwohlbelange dürfen nicht außer Verhältnis stehen zum Eingriff in die informationelle Selbstbestimmung. Dabei kommt es vor allem auf die **Persönlichkeitsrelevanz** der erfaßten Daten oder ihrer Verknüpfungsmöglichkeiten an[55]. Werden Ermittlungen geheim gehalten, erhöht dies die Eingriffsintensität. Heimliche Ermittlungen sind daher nur bei konkreten Verdachtsmomenten , aber nicht anlaßlos oder routinemäßig zulässig.[56]

Videoüberwachung sieht das Bundesverfassungsgericht als intensiven Eingriff an, der weitere belastende Maßnahmen vorbereiten oder das Verhalten von Personen lenken soll. Die Aufzeichnung der Überwachungsdaten erhöht das Gewicht des Eingriffs wegen der Möglichkeit, die Daten auszuwerten, zu bearbeiten und mit anderen Daten zu verknüpfen.[57]

Das Bundesverfassungsgericht schließt nicht aus, daß eine Videoüberwachung öffentlicher Einrichtungen mit Aufzeichnung des gewonnenen Bildmaterials verfassungsgemäß sein kann, wenn für sie ein hinreichender Anlaß besteht und Überwachung sowie Aufzeichnung insbesondere in räumlicher und zeitlicher Hinsicht und im Hinblick auf die Möglichkeit der Auswertung der Daten das Übermaßverbot wahren. Dafür bedarf es allerdings einer hinreichend bestimmten und normenklaren Ermächtigungsgrundlage, die unterscheidet zwischen **Datenerhebung, Datenspeicherung und Datenverwendung** und die zudem die Verhältnismäßigkeit und das Übermaßverbot beachtet. Eine hohe Streubreite mit Einbeziehung von Personen, die keinen Überwachungsanlaß gegeben haben, erhöht die Eingriffsintensität. Überwachungsmaßnahmen müssen räumlich und zeitlich begrenzt sein.[58]

---

[54] z.B. in BVerfG v. 23.02.2007 - 1 BvR 2368/06. B. v. 04.04 2006 - 1 BvR 518/02 -,= NJW 2006, S. 1939,1942, 1944, BVerfGE 100, 313 ; 376, 392; 107, 299 ,320 f.; 109, 279 ,353; 113, 348, 383

[55] BVerfG, B. v., 13.06.2007 - 1 BvR 1550/03 - Kontenabruf

[56] ebd.

[57] BVerfG, B. v. 23.02.2007 - 1 BvR 2368/06 -VÜ Kunst; ähnlich BVerfG, U. v. 11.03.2008 - 1 bvR 2074/05 Kfz-Kennzeichenabgleich

[58] BVerfG, B. v. 23.02.2007 - 1 BvR 2368/06

Die Schutzwirkungen von Grundrechten beziehen sich nicht nur auf die Erhebung, sondern auch auf die **Weitergabe und Verwendung von Daten aus Überwachungsmaßnahmen** und auf datenschutzrechtlichen Vorkehrungen. Bestehen für die Daten*verwendung* keine Sicherungen, ist auch die Daten*erhebung* verfassungswidrig.[59]

Datenspeicherung und Datenverwendung sind an den Erhebungszweck gebunden, eine **Zweckänderung** bedeutet einen eigenständigen Grundrechtseingriff [60]und verlangt daher eine eigenständige Ermächtigungsgrundlage. Die Zweckänderung muß durch hinreichende Allgemeinwohlbelange gerechtfertigt sein, die die grundrechtlich geschützten Interessen überwiegen, sie muß normenklar sein und mit den Aufgaben der Datenempfänger und dem ursprünglichen Verwendungszweck vereinbar sein[61]. Insbesondere darf daher mit der Zweckänderung keine generelle Absenkung der Eingriffsschwelle verbunden sein: die Verwendung setzt einen ähnlich schwerwiegenden Verwendungszweck voraus und zusätzlich eine konkretisierte Verdachtslage. Dürfen die Erkenntnisse bereits im Anlaßverfahren nicht verwertet werden, dann dürfen sie auch nicht weitergegeben werden. Für die wegen des Verhältnismäßigkeitsprinzips notwendige Zweckbindung müssen Daten, die aus besonders schweren Grundrechtseingriffen stammen, besonders **gekennzeichnet** sein, damit bei einer Zweckänderung keine Absenkung des Anlasses für Datenübermittlung und - Verwendung möglich ist. Übermittlungen von Daten aus besonderen Überwachungsmaßnahmen, deren Erhebung an besondere Voraussetzungen geknüpft ist, müssen protokolliert werden.

In der Entscheidung zur Beschlagnahme von Telekommunikations-Verbindungsdaten bei einer Durchsuchung[62] betont das Bundesverfassungsgericht das Recht auf informationelle Selbstbestimmung:

> *„Die freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus“*

und die Gefahren der technischen Entwicklung der Kommunikation und Datenverarbeitung:

> *„Immer mehr Lebensbereiche werden von modernen Kommunikationsmitteln gestaltet. Damit erhöht sich nicht nur die Menge der anfallenden Verbindungsdaten, sondern auch deren Aussagegehalt. Sie lassen in zunehmendem Maße Rückschlüsse auf Art und Intensität von Beziehungen, auf Interessen, Gewohnheiten und Neigungen und nicht zuletzt auch auf den jeweiligen Kommunikationsinhalt zu und vermitteln - je nach Art und Umfang der angefallenen Daten - Erkenntnisse, die an die Qualität eines Persönlichkeitsprofils heranreichen können.“*

Eine solche „Rundumüberwachung“ oder die Erstellung von Persönlichkeitsprofilen verstößt danach gegen die Menschenwürde (Art. 1 Abs. 1 GG).

---

[59] BVerfG v. 03.03.2004 - 1 BvR 2378/98 - Gr. Lauschangriff
[60] BVerfG, B. v. 03.03.2004 -1 BvF 3/92 Außenwirtschaftsgesetz
[61] ebd.
[62] vom 02.03.2006 - 2 BvR 2088/04

Wie schon im Beschluß vom 12. April 2005[63] sieht das Bundesverfassungsgericht dann zwar die gesetzliche Regelung in §§ 94 ff StPO als verfassungskonform an auch für die Beschlagnahme von Datenträgern, die TK-Daten enthalten, aber nur wegen der „strengen Begrenzung aller Maßnahmen auf den Ermittlungszweck". Bei ähnlichen präventivpolizeilichen Regelungen wäre daher die Verfassungsmäßigkeit der gesetzlichen Regelung anders zu beurteilen, wenn nicht ebenfalls ein hochrangiger und gesetzlich genau bestimmter und begrenzter Maßnahmezweck normiert wäre. Im dort entschiedenen Fall war die konkrete Anwendung der gesetzlichen Vorschriften verfassungswidrig.

In der Entscheidung zur Online-Durchsuchung nach dem Verfassungsschutzgesetz NRW[64] definiert das Bundesverfassungsgericht das *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme* als Ausprägung des allgemeinen Persönlichkeitsrechtes, weil der Schutz des Telekommunikationsgeheimnisses in Art. 10 GG, der Schutz der Unverletzlichkeit der Wohnung in Art. 13 GG und das bisher als Ausprägung des Allgemeinen Persönlichkeitsrechtes verstandene Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 GG) dem aus der Entwicklung der Informationstechnik entstandenen Schutzbedürfnis nicht mehr ausreichend Rechnung tragen.

Die Online-Durchsuchung ist ein Grundrechtseingriff von hoher Intensität, denn sie eröffnet einerseits Zugang zu einem umfangreichen Bestand persönlicher Daten, andererseits erfolgt sie durch heimliche Infiltration eines informationstechnischen Systems. Verhältnismäßig kann sie nur sein, wenn

- tatsächliche Anhaltspunkte für
- eine konkrete Gefahr
- für ein überragend wichtiges Rechtsgut vorliegen.

Derart schwere Eingriffe müssen dem Richtervorbehalt unterliegen und durch gesetzliche Ausgestaltung den Kernbereichsschutz gewährleisten[65].

Auch in dieser Entscheidung betont das Bundesverfassungsgericht, daß die Vorverlagerung eines Eingriffs in das Vorfeld konkreter Gefährdungen einerseits, die mögliche Betroffenheit Dritter andererseits die Intensität eines Eingriffs erhöhen und beide nur zulässig sind, wenn dies durch das Gewicht des gefährdeten Rechtsgutes gerechtfertigt ist.

Zufallsfunde aus heimlichen Überwachungsmaßnahmen dürfen nur dann für andere Zwecke, insbesondere für die Aufklärung anderer Taten, verwendet werden, wenn es sich um ähnlich gewichtige Taten oder Gefahren handelt, denn der Verwendungszweck muß mit dem ursprünglichen Überwachungszweck vereinbar sein.[66]

Im Eilbeschluß zur Vorratsdatenspeicherung warnt das Bundesverfassungsgericht vor dem Einschüchterungseffekt, den zu weitgehende Überwachungen auf ndas Verhalten der Bürger haben können.[67]

---

[63] 2 BvR 1027/02 = NJW 2005, S. 1917,1919 f. zur Datenträgerbeschlagnahme
[64] B. v. 27.02.2008 - 1 BvR 370/07
[65] ebd.
[66] BVerfG, U. v. 03.03.2004 - 1 BvR 2378/98 - Gr.Lauschangriff
[67] BVerfG, B.v. 11.03.2008 - 1 BvR 256/08

3 Änderungsbedarf für das Hamburger Polizeirecht

Die Änderungen des hmbSOG und des hmbPolDVG von 2005 umfassen eine Vielzahl sehr unterschiedlicher und teilweise problematischer Änderungen, so z.B.

- eine neue Definition des Begriffs „Straftaten von erheblicher Bedeutung“ in § 1 Abs. 4 PolDVG
- die Ausdehnung der Befugnisse der Polizei „zum Schutz privater Rechte“ in § 1 Abs.3 HmbSOG
- verdachtsunabhängige Eingriffe wie Befragung mit Auskunftspflicht § 3 PolDVG, Identitätsfeststellung § 4 PolDVG
- neue bzw. erweiterte Eingriffsbefugnisse durch technische Mittel wie Videoüberwachung, TKÜ, verdeckte Beobachtung, Großer Lauschangriff, automatische Kennzeichenerfassung, Rasterfahndung (§§ 8 - 10 b 11 - 13 PolDVG)
- erweiterte Befugnisse in der Datenverarbeitung, insbesondere Auflösung der Zweckbindung von Daten (§§ 14, 16 PolDVG)
- erweiterte Zwangsbefugnisse, z.B. Ausdehnung der Dauer des Gewahrsams, des Vollzugs des Gewahrsams in Justizvollzugsanstalten (§ 13 c hmbSOG) und Neuregelung des Schusswaffengebrauches mit Befugnis zum finalen Todesschuss in § 24 ff. hmbSOG
- Einführung neuer Waffen: Elektroschockgerät Taser in § 14 Abs. 4 hmbSOG

Hier können nur exemplarisch einige Änderungen auf ihre Verfassungsmäßigkeit hin untersucht werden.

Zu betonen bleibt, daß das Bundesverfassungsgericht - vor allem in der GPS-Entscheidung[68] - vom Gesetzgeber verlangt, wegen der raschen technischen Entwicklung laufend die Tauglichkeit der technischen polizeilichen Überwachungsmaßnahmen für den angestrebten Erfolg ebenso zu prüfen, wie die Frage, ob die bestehenden verfahrensrechtlichen Vorkehrungen für den Grundrechtsschutz ausreichend sind.

Entsprechende **Evaluierung** für das Hamburger Polizeirecht ist noch nicht bekannt. Sie sollte dringend eingefordert werden.

3.1 Gesetzgebungskompetenz: Vorbeugende Bekämpfung von Straftaten?

§ 1 Abs. 1 S. 2 PolDVG weist der Polizei die Datenverarbeitung zu auch

> *„zur Verhütung von Straftaten und zur Vorsorge für die Verfolgung künftiger Straftaten (vorbeugende Bekämpfung von Straftaten).“*

[68] v. 12.04.2005 - 2 BvR 581/01

Damit geht das PolDVG über die klassische Aufgabenzuweisung der Abwehr von Gefahren hinaus und schließt neben den präventiven Zwecken (künftige) repressive Zwecke mit ein.

Für die **Strafverfolgungsvorsorge** hat der Landesgesetzgeber jedoch nur die konkurrierende Gesetzgebungskompetenz (Art. 74 GG). Das Bundesverfassungsgericht hat die Strafverfolgungsvorsorge dem „gerichtlichen Verfahren“ und der Strafverfolgung und nicht den präventiven Zwecken zugeordnet, so daß der Landesgesetzgeber keine Gesetzgebungskompetenz für diesen Bereich hat, wenn der Bundesgesetzgeber seine Kompetenz ausgeschöpft hat.[69] Es fehlt die Beschränkung „soweit die besonderen Rechtsvorschriften keine abschließenden Regelungen enthalten“[70].

Zu prüfen ist daher, ob und in welchem Umfang das PolDVG wegen Verstoß gegen die Gesetzgebungskompetenz verfassungswidrig ist.

In der Literatur wird unterschieden zwischen den Aufgaben „Gefahrenabwehr“, „vorbeugende Bekämpfung von Straftaten“, „Verhütung von Straftaten“ und „Vorsorge für die Verfolgung künftiger Straftaten“. Teilweise wird die „vorbeugende Bekämpfung von Straftaten“ insgesamt der „Gefahrenabwehr“ zugerechnet, teilweise nur die „Verhütung von Straftaten“, nicht aber die „künftige Straftatenvorsorge“.[71] Mit der Verlagerung der polizeilichen Eingriffsbefugnisse in die Risikovorsorge, also die Vorsorge für künftige Gefahrenabwehr oder künftige Strafverfolgung, verschwimmen die Grenzen von Prävention und Repression, also auch das begrenzende Merkmal der Zweckbestimmung von Daten.

Hinzu kommt, daß im Bereich der „Risikovorsorge“ die Maßnahmen der (heimlichen) Informationsgewinnung „Verdachtsschöpfungs- und Verdachtskonkretisierungsinstrumente“ sind und nicht mehr an einen konkreten Straftatenverdacht oder eine konkrete Gefahr anknüpfen. Damit verschwimmt nicht nur die Grenze zwischen Prävention und Repression, sondern auch andere rechtsstaatliche Begrenzungen - wie das Übermaßverbot oder tatbestandliche Bestimmtheit - verlieren ihre beschränkende Funktion, weil die Eingriffsbefugnis an vage Prognosen statt erhärtete Tatsachen anknüpfen. Die Vorverlagerung der Eingriffsschwelle sollte daher aus rechtsstaatlichen Gründen ohnehin restriktiv gehandhabt werden.[72]

Die Aufgabenzuweisung des § 1 PolDVG und die sonstigen Regelungen des PolDVG umfassen einerseits die Informationsgewinnung mit offenen und heimlichen Datenerhebungseingriffen, andererseits die weitere Verwendung und Verarbeitung von präventiv oder repressiv erhobenen Daten, auch unter Zweckänderung (vgl. §§ 14 ff. PolDVG).

Im Bereich der heimlichen Überwachungsmaßnahmen, also den besonders intensiven Grundrechtseingriffen, gibt es erhebliche Überschneidungen mit den Regelungen in der Strafprozeßordnung, insbesondere für die Überwachung der Telekommu-

---

[69] hierzu s.o. 2.1 und BVerfG, B. v. 27.07.2005 - 1 BvR 668/04 zum NdsSOG/TKÜ

[70] Denninger in Lisken/Denninger, Handbuch des Polizeirechtes, 4. Aufl. 2007, Anm, E 174 unter Verweis auf die Regelungen in § 17 Abs. 2 ASOG Bln, § 10 Abws. 2 S. 2 BremPolG; § 3 Abs. 1 S. 2 NGefAG u.a.

[71] s. hierzu Rachor in Lisken/Denninger, Handbuch des Polizeirechtes, 4. Aufl. 2007, Kap. F Anm. 158 ff. ; Denninger, a.a.O. Kap. E Anm. 199ff.

[72] vgl. hierzu auch Denninger, Handbuch des Polizeirechtes, 4. Aufl. 2007, Kap. E Anm 192 ff

nikation (§§ 100 a, b StPO), optische und akustische Überwachungsmaßnahmen unter Einschluß der Video- und Wohnraumüberwachung („Lauschangriff“, § 100 c StPO) und der Ausforschung der Telekommunikationsverbindungsdaten (§ 100 g StPO). Diese Regelungen sollten die polizeilichen Befugnisse im Bereich der Strafverfolgung nach h.M. abschließend regeln[73]. Damit hat der Bund seine Gesetzgebungskompetenz „zur künftigen Strafverfolgung“ ausgeschöpft und an restriktive Voraussetzungen geknüpft. Es besteht daher - jedenfalls für den Zweck der künftigen Strafverfolgung - keine Gesetzgebungsbefugnis für den Landesgesetzgeber mehr.

Allerdings sehen die Datenverarbeitungsvorschriften der Strafprozeßordnung, aber auch der Landespolizeigesetze, jeweils wechselseitig die Verwendung der Daten vor (z. B. § 100 f Abs. 2 StPO, § 16 Abs. 2 PolDVG). Dies setzt aber voraus, daß die jeweils zu anderen Zwecken übermittelten Daten ursprünglich für einen zulässigen präventiven Zweck von der Polizei oder einen repressiven Zweck von den Strafverfolgungsbehörden erhoben worden sind. Keinesfalls ergibt sich hieraus eine Kompetenzerweiterung.

Die Erhebung von Daten für Zwecke künftiger künftiger Strafverfolgung verstößt nach der Entscheidung des Bundesverfassungsgerichtes zum NdsSOG somit gegen Art. 74 GG und ist daher verfassungswidrig[74]. Die künftige Strafverfolgung muß als Zweck der polizeilichen Datenverarbeitung aus dem Landespolizeirecht gestrichen werden.

Auch im Bereich der weiteren Verwendung von strafprozessual erhobenen Daten für präventive Zwecke gibt es gesetzliche Überschneidungen und damit Probleme der Gesetzgebungskompetenz:

Der Bundesgesetzgeber hat die Datenverarbeitung für die Strafverfolgungsvorsorge auch für künftige Strafverfolgungszwecke geregelt in §§ 483 ff StPO. Insbesondere beschränkt § 484 Abs. 2 StPO die Verarbeitung von Daten, die über die reine Vorgangsverwaltung hinausgehen, auf Daten von Personen, bei denen „wegen der Art oder Ausführung der Tat, der Persönlichkeit des Beschuldigten oder Tatbeteiligten oder sonstiger Erkenntnisse Grund zu der Annahme besteht, daß weitere Strafverfahren gegen den Beschuldigten zu führen sind“.

Allerdings bestimmt § 484 Abs. 4 StPO darüber hinaus, daß das Landespolizeirecht die weitere Verwendung strafprozessual gespeicherter Daten „für Zwecke künftiger Strafverfahren“ regeln kann, „ausgenommen die Verwendung für Zwecke eines Strafverfahrens“. Diese Vorschrift ist nur verständlich für die Rechtslage vor der Entscheidung des Bundesverfassungsgerichtes zum NdsSOG - denn danach sind polizeiliche „Zwecke künftiger Strafverfahren“, die nicht die Vorsorge für künftige Strafverfolgung betreffen, kaum denkbar.

Nach der klaren Abgrenzung durch das Bundesverfassungsgericht kann es allein noch Aufgabe der Landespolizei sein, Gefahren und Straftaten abzuwehren, während alle Datengewinnung und Datenverarbeitung zur Erhärtung eines gegenwärtigen oder künftigen Tatverdachtes zum Strafverfahren, also zur Bundeskompetenz zu rechnen ist.

---

[73] Denninger, a.a.O. Anm. 175
[74] s. hierzu oben unter 2.1

Allerdings schließt das Bundesverfassungsgericht nicht aus, daß sog. Mischdateien unterhalten werden und sowohl zu Strafverfolgungszwecken als auch für präventive Zwecke der Zugriff erfolgt. In einem solchen Fall verlangt allerdings das Gebot der Normenbestimmtheit und Normenklarheit eine eindeutige gesetzliche Bestimmung der Zugriffszwecke.[75] Im konkret entschiedenen Fall des Kfz-Kennzeichenabgleichs war die mangelnde Differenzierung strafverfolgender und gefahrenabwehrender Zwecke ein Grund für die Verfassungswidrigkeit der Ermächtigungsnorm für Datenerhebung und Datenverarbeitung.

Mit der unbegrenzten, nicht an eine konkrete Gefahr oder einen konkreten Straftatenverdacht anknüpfenden Möglichkeit zur Datenverarbeitung über § 484 Abs. 2 StPO hinaus durch die pauschale Aufgabenzuweisung des § 1 Abs. 1 S. 2 hmbPolDVG wird die Möglichkeit zu Eingriffen in das informationelle Selbstbestimmungsrecht ins Uferlose ausgedehnt. Bei der behördenüblichen Speicherung von strafprozessual erhobenen, aber für ein konkretes Strafverfahren nicht mehr benötigten persönlichen Daten durch die Polizei fehlt es zudem auch an der begrenzenden Funktion der Zweckbestimmung. Die ursprüngliche Zweckbestimmung für die Erhebung der Daten - ein konkretes Strafverfahren - hat sich erledigt, mit der weiteren Speicherung ist immer eine Zweckänderung verbunden. Dies bedeutet nach der oben zitierten Rechtsprechung des Bundesverfassungsgerichtes einen neuen Grundrechtseingriff, der eine eigenständige Rechtfertigung und vor allem eine Einzelfallprüfung statt eine automatische Datenübernahme benötigt.

Über das PolDVG werden aber praktisch alle ursprünglich zu Ermittlungszwecken erhobenen Daten in präventiv-polizeiliche Dateien überführt. Eine Prüfung der Notwendigkeit, die wegen der Zweckänderung datenschutzrechtlich geboten ist, findet im Einzelfall praktisch nicht mehr statt.

Dies hat u.a. zur Folge, daß etwa alle Bürger, gegen die ein Ermittlungsverfahren wegen angeblichen Verstoß gegen das Versammlungsgesetz geführt wurde, selbst dann jahrelang in polizeilichen Dateien gespeichert bleiben, wenn sich im Laufe des Verfahrens herausstellt, daß sie zu Unrecht beschuldigt wurden oder daß ihr Verhalten nicht strafbar war, etwa weil es von der Versammlungsfreiheit (Art. 8 GG) gedeckt war. Gleiches gilt für alle eingestellten Ermittlungsverfahren, vor allem wenn der sachbearbeitende Polizist wegen der Art des Deliktes eine künftige Relevanz annimmt, etwa bei (behauptetem aber entkräftetem) Stalking- oder Beleidigungsvorwurf oder Ermittlungsverfahren im politischen Kontext (etwa Hausfriedensbruch oder Nötigung), selbst wenn das Ermittlungsverfahren ergeben hat, daß der Straftatbestand nicht erfüllt war. Ist aber kein strafbares Verhalten vorhanden, kann sich daraus auch kein Gefahr künftiger Straftatenbegehung ergeben.

Derartige Datenspeicherung zu veränderten Zwecken bedürfen nach der Rechtsprechung des Bundesverfassungsgerichtes aber in jedem Einzelfall einer Prüfung der Verhältnismäßigkeit, die zur Zeit nicht gewährleistet ist.

Die unklare gesetzliche Regelung in § 484 Abs. 4 StPO wird ergänzt durch § 14 PolDVG (Zweckbindung) und § 16 PolDVG (Speichern, Ändern, Nutzen von Daten).

---

[75] BVerfG, U. v. 11.03.2008 - 1 BvR 2074/05 - Kfz-Kennzeichenabruf; so auch Petri in Lisken/Denninger, Handbuch des Polizeirechtes, 4. Aufl. 2007, Kap. H Anm. 27, der auch darauf hinweist, daß die generalklauselartige Ermächtigung zur Datenverarbeitung zur Straftatenvorsorge gegen wegen mangelder Normenbestimmheit verfassungsrechtlich bedenklich sind.

Darin wird der Polizei gestattet, - trotz Zweckänderung! - Daten weiter zu verarbeiten „zur Erfüllung ihrer Aufgaben“. Eben diese sind in § 1 Abs. 1 PolDVG zu weit gefaßt, so daß auch Daten zu weitgehend weiter verarbeitet werden dürfen, wenn sich der ursprüngliche Zweck eines konkreten Ermittlungsverfahrens erledigt hat.

§ 16 Abs. 2 PolDVG gestattet denn auch die weitere Verarbeitung von Daten, die bei der Strafverfolgung gewonnen wurden, **uneingeschränkt** für Zwecke der Gefahrenabwehr. Lediglich mit besonderen Methoden erhobene Daten unterliegen Beschränkungen bei der weiteren Verwendung.

Problematisch ist ebenso die Befugnis in § 16 Abs. 3 PolDVG zur Datenverarbeitung betreffend Kontaktpersonen „zur vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung“, wegen eben derselben Kompetenzüberschneidung mit dem Bundesgesetzgeber.

Bisher ist die Problematik der Verfassungsmäßigkeit von § 484 Abs. 4 StPO i.V.m. den komplementären Regelungen im Landespolizeirecht noch nicht von den Instanzgerichten erörtert worden. Diese setzen sich bislang nur mit dem zulässigen Rechtsweg bei Doppelspeicherungen auseinander.

Die Frage, ob § 484 StPO insoweit eine abschließende Regelung enthält oder ob der Bundesgesetzgeber mit § 484 Abs. 4 StPO die Öffnung für weitergehende Regelungen des Landesgesetzgebers im Rahmen der konkurrierenden Gesetzgebungskompetenz zulassen wollte, ist komplex und sollte gesondert untersucht werden.

3.2 Normenklarheit, Normenbestimmtheit

Die gesetzliche Systematik des hmbSOG und PolDVG ist unübersichtlich. Eingriffsbefugnisse und die ihre Grenzen bestimmenden gesetzlichen Voraussetzungen sind verwischt. Es wird zu viel mit Querverweisungen und nur scheinbar befugnisbegrenzenden Katalogen gearbeitet.

Das hmbSOG und PolDVG sollten komplett neu gefaßt werden, um wieder eine Übersichtlichkeit und Anwendungstauglichkeit zu erlangen. Mit der vorhandenen Regelung mit Scheinbegrenzungen und anschließenden Ausnahmen ist kaum konkret zu bestimmen, wo die polizeiliche Befugnis beginnt und endet.

Polizeiliche Eingriffsbefugnisse in die Grundrechtssphäre sollten im SOG übersichtlich und vollständig geregelt werden, das hmbSOG und das PolDVG sollten wieder in ein Gesetz zusammengeführt werden, wie dies schon 2005 vom Landesdatenschutzbeauftragten gefordert wurde.[76] Das Gesetz würde an Übersichtlichkeit gewinnen, wenn Regelungen wie etwa der Kernbereichs- und Berufsschutz oder die Inanspruchnahme von Kontaktpersonen und Dritter „vor der Klammer“ in eigenen Para-

[76] Landesbeauftragter für den Datenschutz in der Anhörung von Innenausschuß und Rechtsausschuß in der Hamburger Bürgerschaft vom 18.02.2005, Drs. 18 /12

graphen geregelt werden würde[77], statt in langen Ausführungen bei jeder einzelnen Eingriffsbefugnis wortgleich oder leicht im Wortlaut voneinander abweichend.

Generalklauselartige Ermächtigungen zu Datenerhebung und Datenverarbeitung verstoßen gegen die Grundsätze der Normenbestimmheit und Normenklarheit sowie gegen den Verhältnismäßigkeitsgrundsatz. Eingriffe in das informationelle Selbstbestimmungsrecht sind umso intensiver, je verdachtsunabhängiger die Datenerhebung und weitere Datenverarbeitung erfolgt, und je größer die automatisierten Verknüpfungs- und Zugriffsmöglichkeiten sind. Je intensiver der Eingriff, umso genauer müssen Datenerhebungsbefugnisse und die Befugnisse zu Datenspeicherung, Datenabruf und - übermittlung, Datenabgleich und Zweckveränderung detailliert in der gesetzlichen Ermächtigung geregelt werden. Daran mangelt es im PolDVG.

3.2.1 Datenerhebung im öffentlichen Raum § 8 PolDVG

So geht es in § 8 PolDVG um die Befugnis zur „Datenerhebung im öffentlichen Raum und an besonders gefährdeten Objekten“. In 7 Absätzen werden dann sehr unterschiedliche Eingriffsbefugnisse geregelt, wie die (verdeckte) Anfertigung von Bild- und Tonaufnahmen bei öffentlichen Veranstaltungen (Abs. 1) oder an „gefährdeten Orten“ (Abs. 2) gegen (potentielle) Störer und Dritte, die offene verdachts- und gefahrunabhängige Videoüberwachung von Orten (Abs. 3), die Videoüberwachung von Festgenommenen (Abs. 4) , die Videoüberwachung an Kontrollstellen (Abs. 5) und der automatische Kennzeichenabgleich (Abs. 6).

Die gesamte Vorschrift ist ein Katalog von Erlaubnissen zur technischen Überwachung von „jedermann“ - eingriffsbegrenzende Tatbestandsvorausssetzungen findet man nur mit Mühe.

In Abs. 1 sind dies „über die für eine Gefahr Verantwortlichen“, „wenn Tatsachen die Annahme rechtfertigen“ „dass dabei Straftaten begangen werden“. Der betroffene Bürger und die „Gefahr“, nämlich Straftaten zu verhindern, benötigen noch nicht einmal einen Zusammenhang; der scheinbar angenommene Zusammenhang wird sogleich wieder aufgehoben durch „wenn Dritte unvermeidbar betroffen werden“. Die Daten dürfen dann nicht nur „zur Strafverfolgung“ , sondern - entgegen der scheinbar eingrenzenden Beschränkung der Abwehr von Straftaten - auch zur Verfolgung von „Ordnungswidrigkeiten von erheblicher Bedeutung“ oder für die „künftige Strafverfolgung“ oder „zur vorbeugenden Bekämpfung von Straftaten“ gespeichert und verwendet werden, und - über die Verweisung in Abs. 7 - auch zur Aus- und Fortbildung sowie zu statistischen Zwecken (§ 17 PolDVG) und zur Forschung (§ 24 Abs. 4 PolDVG).

Begrenzende Tatbestandsmerkmale wie etwa eine qualifizierte Gefahr (konkrete, gegenwärtige, unmittelbare, erhebliche Gefahr oder Gefahr für bestimmte herausragende Rechtsgüter) sucht man ebenso vergeblich wie die Beschränkung der Dateneingriffe auf „Störer“ oder „Verantwortliche“ und darüber hinaus nur bei gesteigerten Gefahren für gravierende Rechtsgüter.

---

[77] s. hierzu Roggan, Stellungnahme zur Änderung des HessSOG, Ausschußvorlage INA 173/3 Nr. 6 , S. 46 unter Hinweis auf Zöller StraFo 2008, 21 f. und zur Regelung im Brandenburgischen Polizeigesetz

Diese mangelhafte Gesetzgebungstechnik zieht sich durch die gesamte Neuregelung von 2005. Ähnlich unübersichtlich und nur scheinbar begrenzend ist die Regelung zur optischen und akustischen Wohnraumüberwachung in § 10 PolDVG, die Regelungen zur Telefon- und Verkehrsdatenüberwachung und die Datenverarbeitungsvorschriften insgesamt.

3.2.2. Straftaten von erheblicher Bedeutung

§ 1 Abs. 4 PolDVG in der Fassung von 2005 definiert den Begriff „Straftaten von erheblicher Bedeutung". Es handelt sich um eine Scheindefinition, denn weder handelt es sich um einen abschließenden Katalog von Straftatbeständen, noch wird im Hinblick auf betroffene Rechtsgüter differenziert.

Die „vor die Klammer gezogene" Definition bewirkt, daß schwere Eingriffe in die Individualrechtssphäre auch bei einem relativ leichten Anlaß möglich sind.

§ 100 a StPO arbeitet beispielsweise mit einem besonderen Katalog gemeinschaftsschädlicher oder erheblich individualrechtsschädlicher Straftatbestände, um die Voraussetzung für Telefonüberwachung und andere schwere und heimliche Eingriffsmaßnahmen zu bestimmen.

Demgegenüber umfaßt die Definition in § 1 Abs. 4 PolDVG auch Bagatellkriminalität, nämlich wenn sie „gewerbs-, gewohnheits-, serien- oder bandenmäßig oder sonst organisiert begangen werden" (§ 1 Abs. 4 Ziff. 2 c), wie etwa Taschendiebstahl , Beschaffungskriminalität oder Drogenkriminalität im geringfügigen Bereich.

Praktisch wird diese Definition für die Bestimmung von „gefährlichen Orten" in § 3 Abs. 1 Ziff. 2 a und Abs. 2 PolDVG als Eingriffsschwelle für die verdachtsunabhängige Identitätsfeststellung, als Eingriffsvoraussetzung für die längerfristige Observation (§ 9 Abs. 1 Ziff 2 PolDVG) und über die Verweisung auch für die optische und akustische Überwachung in § 10 Abs. 1 PolDVG. Weiter ist bei Straftaten von erheblicher Bedeutung der Einsatz verdeckter Ermittler zulässig (§ 12 Abs. 1 Ziff. 2 PolDVG) und die Ausschreibung zur polizeilichen Beobachtung (§ 13 Abs. 1 Ziff. 2 PolDVG). Diese Begriffsbestimmung ist damit die „Eintrittskarte" für besondere verdachtsunabhängige oder heimliche Eingriffsakte.

Während im übrigen schwerere Eingriffe in der Systematik des hmbSOG gefahr- und rechtsgutbezogen definiert werden (Gefahr für Leib und Leben, unmittelbare Gefahr, schwere Gefahr etc.), faßt der Begriff „Straftaten von erheblicher Bedeutung" verschiedene Kriterien zusammen, die besser getrennt bleiben. „Vergehen" erhalten die Eigenschaft durch die Wertung, sie seien „im Einzelfall besonders geeignet, den Rechtsfrieden zu stören". Damit übernimmt nicht mehr der Gesetzgeber selbst, sondern erst der polizeiliche Rechtsanwender die Bestimmung der tatbestandlichen Eingriffsschwelle für verdachtsunabhängige Kontrollen oder heimliche Eingriffsakte.

Nach dem vorgesagten muß aber die Begriffsbestimmung gerade von Zweck und Grenzen des Eingriffs für Bürger und Rechtsanwender *aus dem Gesetz selbst* erkennbar sein, möglichst ohne schwer verständliche Querverweisungen.

Die Begriffsbestimmung in § 1 Abs. 4 PolDVG sollte auf wenige schwere Delikte zurückgeführt werden. Bagatelldelikte sollten keine verdachtsunabhängigen Vorfeldkontrollen ermöglichen. Vor allem aber sollten die Eingriffsschwellen für Observationen, den verdeckten Einsatz technischer Mittel und den Einsatz verdeckter Ermittler auf die Störer einer „unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person“ begrenzt werden (wie in § 9 Abs. 1 Ziff. 1, 10 Abs. 1 S. 1 , 12 Abs. 1 Ziff. 1 PolDVG).

Das Bundesverfassungsgericht hat in seiner Entscheidung zur GPS-Überwachung nach § 100 c Abs. 1 Nr. 1 Buchstabe b StPO das Merkmal der **„Straftat von erheblicher Bedeutung**“ als Rechtfertigung für erhebliche Grundrechtseingriffe im Strafverfahren wie folgt bestimmt:

> *Eine solche Straftat muss mindestens dem Bereich der mittleren Kriminalität zuzurechnen sein, den Rechtsfrieden empfindlich stören und dazu geeignet sein, das Gefühl der Rechtssicherheit der Bevölkerung erheblich zu beeinträchtigen.*[78]

Da auch im Hamburger Polizeirecht das Merkmal „Straftat von erheblicher Bedeutung“ im wesentlichen dazu dient, Eingriffe mit erheblicher Eingriffsintensität zu ermöglichen, muß - wegen der Verhältnismäßigkeit - entweder der Begriff ebenso restriktiv definiert werden oder es müssen bei jeder Einzelbefugnis Katalogtaten mit erheblichem Gewicht einzeln definiert werden.

In der geltenden Fassung sind die Eingriffsschwellen für die genannten Befugnisse zu gering und verstoßen gegen das Prinzip der Verhältnismäßigkeit. Die genannten Regelungen verstoßen auch gegen das Bestimmtheitsgebot.

3.3 KFZ-Kennzeichenabgleich § 8 Abs. 6 PolDVG

§ 8 Abs. 6 PolDVG regelt den Automatischen Kfz-Kennzeichenabgleich:

> *„Die Polizei darf 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 automatisierten Abgleichs mit dem Fahndungsbestand erheben. Daten, die im Fahndungsbestand nicht enthalten sind, sind unverzüglich zu löschen.“*

Diese Vorschrift ist nach der Entscheidung des Bundesverfassungsgerichtes zum Kfz-Kennzeichenabgleich in Hessen und Schleswig-Holstein vom 11.03.2008 - 1 BvR 2074/05 und 1 BvR 1254/07[79] **verfassungswidrig**. [80]Dort hat das Bundesverfassungsgericht ausgeführt:

---

[78] v. 12.04.2005 - 2 BvR 581/01 unter Hinweis auf BVerfGE 103, 21,34; 107, 299,322; 109, 279, 344

[79] = NJW 2008, 1505

[80] so schon der LfD Lubomierski in einer Pressemeldung vom 11.03.2008

„Die bloße Benennung des Zwecks das Kraftfahrzeugskennzeichen mit einem gesetzlich nicht näher definierten Fahndungsbestand abzugleichen, genügt den Anforderungen an die Normenbestimmtheit nicht.
Die automatisierte Erfassung von Kraftfahrzeugkennzeichen darf nicht anlaßlos erfolgen oder flächendeckend durchgeführt werden. Der Grundsatz der Verhältnismäßigkeit im engeren Sinne ist im Übrigen nicht gewahrt, wenn die gesetzliche Ermächtigung die automatisierte Erfassung und Auswertung von Kraftfahrzeugkennzeichen ermöglicht, ohne dass konkrete Gefahrenlagen oder allgemein gesteigerte Risiken von Rechtsgutgefährdungen oder - verletzungen einen Anlaß zur Einrichtung der Kennzeichenerfassung geben…“

Nach dieser Entscheidung gelten folgende Anforderungen an die gesetzliche Ermächtigung zur Einführung von Automatischen Kennzeichenlesesystemen (AKLS):

- Eine automatisierte Erfassung von Kraftfahrzeugkennzeichen zwecks Abgleichs mit dem Fahndungsbestand greift dann, wenn der Abgleich nicht unverzüglich erfolgt und das Kennzeichen nicht ohne weitere Auswertung sofort und spurenlos gelöscht wird, in den Schutzbereich des Grundrechts auf informationelle Selbstbestimmung (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) ein.

- Die verfassungsrechtlichen Anforderungen an die Ermächtigungsgrundlage richten sich nach dem Gewicht der Beeinträchtigung, das insbesondere von der Art der erfaßten Informationen, dem Anlaß und den Umständen ihrer Erhebung, dem betroffenen Personenkreis und der Art der Verwertung der Daten beeinflußt wird.

- Die bloße Benennung des Zwecks, das Kraftfahrzeugkennzeichen mit einem gesetzlich nicht näher definierten Fahndungsbestand abzugleichen, genügt den Anforderungen an die Normenbestimmtheit nicht.

- Die automatisierte Erfassung von Kraftfahrzeugkennzeichen darf nicht anlaßlos erfolgen oder flächendeckend durchgeführt werden.

- Der Grundsatz der Verhältnismäßigkeit im engeren Sinne ist nicht gewahrt, wenn die gesetzliche Ermächtigung die automatisierte Erfassung und Auswertung von Kraftfahrzeugkennzeichen ermöglicht, ohne daß konkrete Gefahrenlagen oder allgemein gesteigerte Risiken von Rechtsgutgefährdungen oder -verletzungen einen Anlaß zur Einrichtung der Kennzeichenerfassung geben. Die stichprobenhafte Durchführung einer solchen Maßnahme kann gegebenenfalls zu Eingriffen von lediglich geringerer Intensität zulässig sein.

Die Daten, die mit automatisierter Kennzeichenerfassung erhoben werden dürfen, müssen vom Gesetzgeber definiert werden, insbesondere ob ausschließlich das Kennzeichen oder weitere Daten wie Ort, Tag, Uhrzeit der Maßnahme, Fahrtrichtung des Fahrzeuges, erhoben werden dürfen. Aus Gründen der Verhältnismäßigkeit bedarf es bei einem solchen Eingriff mit erheblicher Streubreite einer Eingriffschwelle wie „gegenwärtige Gefahr“ oder „gegenwärtige Gefahr für gewichtige Rechtsgüter“. Der Zweck der Maßnahme muß geregelt sein.

Der Landesgesetzgeber hat nicht die Befugnis zur repressiven Datenerhebung (zur Strafverfolgung), sondern nur für präventive Zwecke[81]. Daher muß auch gesetzlich geregelt werden, mit welchen Datenbeständen ein Abgleich erfolgen soll. Der Landesgesetzgeber darf nur den Abgleich mit präventiven Dateien bestimmen.

Bewegungs- und Persönlichkeitsbilder müssen zuverlässig ausgeschlossen werden. „Nichttreffer" sind durch technische Vorkehrungen sofort und anonym zu löschen.

Die automatische Kennzeichenerfassung ist ein schwerwiegender Grundrechtseingriff schon wegen der großen Streubreite, die ein Gefühl des Überwachtwerdens und Einschüchterungseffekte hervorrufen kann mit der Folge von Beeinträchtigung bei Grundrechtsausübung und negativen Auswirkungen für individuelle Entfaltungschancen als auch für das Gemeinwohl. Dies gilt insbesondere beim Kennzeichenabgleich im Zusammenhang mit Versammlungen, die dem Schutz des Art. 8 Abs. 1 GG unterliegen.[82]

Umgekehrt ist der Nutzen der Kennzeichenlesesystem sehr zweifelhaft: Untersuchungen in Bayern und Hessen ergaben eine Trefferquote von 0,03%, in Mecklenburg-Vorpommern wurden sie ausschließlich gegen G8-Proteste eingesetzt mit lediglich 4 Trefferfällen ohne weitere Folgemaßnahmen und auch in Brandenburg nur im Vorfeld von Versammlungen[83].

Der schleswig-holsteinische Innenminister hat sich nach der Entscheidung des Bundesverfassungsgerichtes gegen eine erneute Kennzeichenerfassungsregelung ausgesprochen wegen eines Mißverhältnisses zwischen Aufwand und Ertrag. Seit Beginn der Erprobungshphase August 2007 bis 11.03.2008 wurden lediglich 26 Verstöße gegen das Haftpflichtversicherungsgesetz festgestellt (geringfügiges Delikt), kein einziges gestohlenes Fahrzeug hat sich unter den ca. 131.000 erfaßten Kennzeichen befunden. Daher ist Kfz-Scanning ein ungeeignetes Instrument zur Abwehr von Gefahren und bindet Personal, das an anderer Stelle sinnvoller für operative Polizeiarbeit eingesetzt werden kann.[84] Auch Bremen hat inzwischen auf den Kennzeichenabgleich verzichtet[85].

Hamburg sollte die Vorschrift ersatzlos streichen.

3.4 Videoüberwachung § 8 PolDVG

Zur Videoüberwachung wird auf das gesonderte Gutachten von Rechtsanwalt Carsten Gericke verwiesen. Danach ist die Regelung der Videoüberwachung in § 8

---

[81] so auch Roggan, Stellungnahme für den Innenausschuss des Hessischen Landtages, Ausschussvorlage INA 17/3 Teil 1 Nr. 6

[82] Mecklenburg-Vorpommern hat AKLS nur im Zusammenhang mit G 8-Protesten benutzt. Auf dieses Problem weist auch Roggan hin in der Stellungnahme für den Innenausschuss des Hessischen Landtages, Ausschussvorlage INA 17/3 Teil 1 Nr. 6

[83] alle Angaben nach Breyer, Stellungnahme zum Novellierung des HessSOG für den Innenausschuss des Hessischen Landtages, Ausschussvorlage INA 17/03 Teil 1 Nr. 12 S. 130 f m.w.N.

[84] Unabhängiges Landesamt für den Datenschutz Schleswig-Holstein, Stellungnahme zur Novellierung des HessSOG für den Innenausschuss des Hessischen Landtages, Ausschußvorlage INA 17/3 Teil 1 Nr. 10.

[85] http://www.bremische-buergerschaft.de/drucksachen/190/4421_1.pdf

PolDVG im Hinblich auf Datenerhebung verfassungswidrig wegen mangelnder Bestimmtheit, zudem wegen unverhältnismäßiger Eingriffe in die Grundrechte der Anwohner und Anlieger und schließlich im Hinblick auf die Datenspeicherung für Strafverfolgungszwecke wegen mangelnder Gesetzgebungskompetenz.

Hinzu kommt, daß erhebliche Gründe dafür sprechen, daß die Videoüberwachung **untauglich** ist zur Kriminalitätsverhütung, jedenfalls ihre Evaluierung noch aussteht. Erfüllt die Videoüberwachung nicht die Erwartungen, wegen derer sie eingeführt würde, könnte die Maßnahme auch verfassungswidrig sein, weil sie dann unverhältnismäßig in das informationelle Selbstbestimmungsrecht der Bürger eingreift, ohne daß auf der anderen Seite ein legitimer präventivpolizeilicher Zweck erreicht wird.

Ergänzend wird hier daher auf die Studie des britischen Innenministeriums[86] verwiesen. In Großbritannien arbeiten flächendeckend 4 Mio. Kameras - die Studie kommt zum Ergebnis, daß die Videoüberwachung weitgehend wirkungslos ist. Es kommt zu Fehlern in der technischen Umsetzung und bei der Installation. Manche Kameras stehen an sinnlosen Standorten, mit Sichthindernissen oder Belichtungsfehlern. Die Ansprüche an die Technologie bei ihrer Einführung waren überhöht, Videoüberwachung ist kein Allheilmittel gegen so unterschiedliche Delikte wie Diebstahl, Einbruch, Überfälle, Sachbeschädigung, Vandalismus, Drogenhandel, illegales Müllabladen oder Störungen der öffentlichen Ordnung. Eine hohe Fehlerquelle ist der Faktor Mensch: es gibt wesentlich weniger Monitore als Überwachungskameras, häufig keine zeitgleichen Bilder, ein Hilfspolizist muß viele Monitore und Kameras überwachen. Die Einschätzung der Wichtigkeit, worauf sich die Überwachung am Monitor fokussiert, beruht häufig auf Vorurteilen (86 % der beobachtete Zielpersonen sind junge Leute unter 30, 93 % männlich, Schwarze haben ein doppelt so hohes Überwachungsrisiko) [87].

Die Rentabilität der VÜ ist gering: bei 900 gezielten Observierungen kam es nur 45 Mal zum Einschreiten und nur zu 12 Festnahmen. In Glasgow sahen die Kameras weniger als 5 % der Vorfälle, die in ihrer Überwachungszone zu Festnahmen geführt haben.

Die Wirkung der VÜ setzt voraus, daß die Bilder zeitgleich auf Monitoren überwacht werden, daß es einen guten Informationsfluß zwischen Kontrollraum und Vollzugspolizei sowie eine sofortige Reaktion der Vollzugspolizei gibt. Die Tauglichkeit für die nachträgliche Verwendung als Beweismittel hängt von den Speicherkapazitäten ab[88] (und ist in der Bundesrepublik ein Problem der konkurrierenden Gesetzgebung für die Strafverfolgung).

Die britische Studie konnte keinen Zusammenhang zwischen Aufklärungsrate und Anzahl der Kameras feststellen, obwohl in Großbritannien auf 14 Einwohner eine Überwachungskamera kommt - „ein vollständiges Fiasko“[89].

---

[86] Gill/Spriggs, Assessing the impact of CCTV, UK Home Office Research Study Nr. 292, London Febr. 2005

[87] Norris/Armstron, CCTV and the Social Structuring of Surveillance, in: Crime Prevention Studies, Vol.10 London 1999

[88] Noé Leblanc, Big Brother ist kurzsichtig - der zweifelhafte Nutzen von Überwachungskameras, Le monde diplomatique, September 2008, S. 19

[89] Chief Inspector Mick Neville, London Metropolitan Police, in The Guardian, 06.05.2008

3.5 Lausch- und Spähangriff, Wohnraumüberwachung § 9 PolDVG

§ 9 PolDVG fasst die Observation mit optischen und akustischen Mitteln (Lausch- und Spähangriff) und die Wohnraumüberwachung in einem Paragraphen zusammen, in einer unübersichtlichen Gesetzgebungstechnik mit Verweisungen schon für die tatbestandliche Voraussetzung der Eingriffsermächtigung

> *„…unter den Voraussetzungen des § 9…“*.

3. 5. 1 Normenbestimmtheit, Normenklarheit, Verhältnismäßigkeit

Dies begegnet Bedenken im Hinblick auf **Normenbestimmtheit und Normenklarheit** und sollte so verändert werden, daß die Voraussetzungen der Eingriffsermächtigung (zum Schutz welcher Rechtsgüter, auf welcher Verdachts- oder Tatsachenbasis, bei welcher Gefahrenintensität, gegen Verantwortliche oder auch gegen Dritte, als ultima ratio) aus der Regelung selbst zu ersehen sind. In der gegenwärtigen Fassung ist auch die Verhältnismäßigkeit von Eingriffsintensität und Anlaß nicht gewahrt.

Verfassungswidrig ist die Unbestimmtheit der Eingriffsschwelle, denn das Bundesverfassungsgericht verlangt in der Entscheidung zum Großen Lauschangriff [90] und in der Entscheidung zur akustischen Wohnraumüberwachung nach § 100 c StPO[91] klare und eindeutige Vorgaben durch den Gesetzgeber, die der hohen Eingriffsintensität der Wohnraumüberwachung gerecht werden.

Art. 13 Abs. 3 GG gestattet die Wohnraumüberwachung nur zur Abwehr *von im Gesetz selbst bestimmten schweren Straftaten,* wenn es einen *auf Tatsachen begründeten Verdacht* gibt und *andere Mittel ausgeschöpft sind:*

> *„Dadurch wird im Verfassungstext selbst klargestellt, daß die Abhörmaßnahme als besonders schwerer Eingriff in das Grundrecht auf Schutz der Wohnung ultima ratio der Strafverfolgung ist. Die Überwachung einer Wohnung kommt im Übrigen nur in Betracht, wenn und solange der Beschuldigte sich vermutlich in ihr aufhält.“* .[92]

Diese Voraussetzungen muß eine gesetzliche Regelung aufgreifen und ausgestalten. Daran mangelt es in § 10 PolDVG.

3.5.2 Grundrechtsschutz durch Verfahren

Der „einfache“ Lausch- und Spähangriff unterliegt weder einem Richter- noch Behördenleitervorbehalt, die Verweisung auf die Voraussetzungen der Observation umfaßt nicht den Behördenleitervorbehalt des § 9 Abs. 2 PolDVG.

Die Wohnraumüberwachung steht unter Richtervorbehalt (§ 10 Abs. 3 PolDVG), bei Gefahr im Verzug unter Behördenleitervorbehalt. Behördenleiter- und Richtervorbe-

---

[90] v. 03.03.2004 - 1 BvR 2138/98
[91] v. 11.05.2007 - 2 BvR 543/06
[92] BVerfG, B. v. 03.03.20094 - 2138/98

halt gelten nicht bei Schutzmaßnahmen für Polizeibeamte im Einsatz (§ 10 Abs. 4 PolDVG), obwohl nicht ersichtlich ist, warum in einem solchen Fall das Schutzbedürfnis der Betroffenen geringer sein soll.

Verwertungsverbote und Löschungspflichten sind in § 10 Abs. 4 ungenügend geregelt.

Verfassungswidrig ist jedenfalls der Einsatz technischer Mittel in Wohnungen zum Schutz von Polizisten im Einsatz ohne Richtervorbehalt nach § 10 Abs. 4 PolDVG wegen Verstoß gegen den Richtervorbehalt in Art. 13 und Art. 10 Abs. 4 GG.

3.5.3. Kernbereichsschutz, Berufsschutz

Der Kernbereichsschutz in § 10 Abs. 5 PolDVG ist ungenügend:

Die Kennzeichnungspflicht ist zwar begrüßenswert, sie hat aber keine praktischen Auswirkungen auf Verwertungsverbote und Löschungspflichten. Alle Daten dürfen ausgewertet werden, es fehlt die Pflicht zum Abbruch, sobald sich herausstellt, daß der private Kernbereich tangiert ist. Es fehlen absolute Erhebungs- und Verwendungsverbote. Die Vorschrift ist daher verfassungswidrig.

Der Berufsschutz außerhalb des privaten Kernbereichs eist ausreichend, weil Überwachungsergebnisse aus geschützten beruflichen Vertrauensverhältnissen bereit einem Erhebungsverbot unterliegen (§ 10 Abs. 2 a PolDVG) und Zufallsfunde zudem einem Verwendungsverbot (§ 10 Abs. 5 S. 3 PolDVG).

3.5.4. Anforderungen an eine Neuregelung

Vor einer Neuregelung ist die **Notwendigkeit der präventiven Wohnraumüberwachung generell zu prüfen**, denn für schwere Straftaten, versuchte Straftaten, geplante Verbrechen (§ 30 StGB) und Vereinigungsdelikte (§§ 129, 129 a StGB) bestehen ausreichende Befugnisse in der Strafprozeßordnung (§ 100 c, d StPO). Jenseits derart konkreter schwerwiegender Straftaten ist die Notwendigkeit nicht ersichtlich - bei Beachtung der Vorgaben des Bundesverfassungsgerichtes zu Eingriffsvoraussetzungen und Kernbereichsschutz verbleibt kaum noch ein denkbarer Anwendungsbereich[93]. Gibt es keinen präventiven Anwendungsbereich, können Lausch- und Spähangriffe sowie Wohnraumüberwachung ersatzlos gestrichen werden[94].

§ 10 Abs. 8 PolDVG normiert die Unterrichtungspflicht des parlamentarischen Kontrollgremiums. Anhand der somit vorhandenen Daten ist die Notwendigkeit einer präventiven Wohnraumüberwachung jenseits der Befugnisse nach der StPO zu prüfen.

---

[93] so auch Breyer, Stellungnahme zur Neuregelung des HessSOG im Innenausschuss des Hessischen Landtages, INA 17/3 Teil 1 Nr. 12, S. 11; das Max-Planck-Institut für deutsches und internationales Strafrecht stellte schon 2004 in einer Untersuchung fest, dass die Fallzahlen und der Ertrag 1998 bis 2003 gering waren, s. Meyer-Wieck, Rechtswirklichkeit und Effizienz der akustischen Wohnraumüberwachung (Großer Lauschangriff) nach § 100 c Abs. 1 Nr. 3 StPO, www.mpicc.de, S. 26 ff., 35, 38

[94] so auch Hilbrans, Stellungnahme zur Neuregelung des HessSOG im Innenausschuss des Hessischen Landtages, INA 17/ 3 Teil 3 Nr. S. 11

Im Polizeirecht darf ein Lauschangriff nur Gespräche betreffen, die Angaben über dringende Gefahren für die öffentliche Sicherheit im Sinne des Art. 13 Abs. 4 GG enthalten.

Der vom Bundesverfassungsgericht verlangte Kernbereichsschutz verlangt ein zweistufiges Schutzkonzept: Die Erhebung kernbereichsrelevanter Daten muß ermittlungstechnisch möglichst unterbleiben, daher muß vor Beginn der Maßnahme eine Prognose erstellt werden[95]. Stellt sich dennoch heraus, daß der private Kernbereich betroffen ist, muß die Maßnahme abgebrochen werden. Für die zweite Stufe sind daher Verfahrensregelungen ausreichend, wenn sich die Kernbereichsrelevanz der erhobenen Daten vor oder bei der Datenerhebung nicht klären läßt. Bei Wohnraumüberwachung muß der Kernbereichsschutz immer in der vorherigen Prognose wahrgenommen werden nach der Art der zu überwachenden Räumlichkeiten oder aus dem Kreis der sich dort befindenden Personen. Wie bei § 100 c Abs. 5 StPO ist auch im Polizeirecht der Kernbereichsschutz „im Ansatz abwägungsfest“ und darf nicht zum Schutz hochrangiger Rechtsgüter beeinträchtigt werden[96] Eine Ermächtigung im Polizeigesetz braucht zudem Löschungspflichten und eine Regelung zur Dokumentation der Löschung. Kernbereichsdaten müssen unverzüglich gelöscht werden, aber die Tatsache der Erfassung der Daten und ihre Löschung sind zu dokumentieren.[97] Weiter müssen Verwendungsverbote bei Kernbereichsverletzungen gesetzlich normiert sein, sowie Benachrichtigungspflichten für alle Betroffenen.

Bei Berufsgeheimnisträgern kann sich der Schutz der Kommunikation aus dem Kernbereich der privaten Lebensgestaltung ergeben, so sind dies etwa seelsorgerische Gespräche mit Geistlichen, Gespräche mit dem Strafverteidiger und Arztgespräche, dagegen nicht Presseangehörige und Parlamentsabgeordnete. Der einfache Gesetzgeber kann aber ein generelles Erhebungsverbot bei allen Berufsgeheimnisträgern normieren. Bei diesen Berufsgeheimnisträgern geht der Schutz soweit, bis konkrete Anhaltspunkte dafür bestehen, daß Gesprächsinhalte zwischen Beschuldigten und Personen keinen absoluten Schutz erfordern, etwa bei Gefährdung von Würde und Leben Dritter, der konkrete Verdacht muß schon beim Zeitpunkt der Anordnung entstehen und kann nicht erst durch eine akustische Wohnraumüberwachung begründet werden. Bei der präventiven Überwachung bedeutet dies, daß Gespräche mit Kernbereichsbezug nur abgehört werden dürfen, wenn die Vertrauensperson selbst an der Straftat beteiligt ist oder Angaben zur Abwehr einer dringenden Gefahr für Würde und Leben Dritter erwartet werden oder wenn das Gespräch mit einem Berufsgeheimnisträger nicht beruflich veranlaßt ist.

3.6 Präventive Rasterfahndung § 23 PolDVG

Rasterfahndung ist ein heimliches Einsatzmittel mit hoher Streubreite und hoher Eingriffsintensität.

---

[95] BVerfG, U. v. 03.03.2004 - 1 BvR 2378/98 Gr. Lauschangriff

[96] Petri in Lisken/Denninger, Handbuch des Polizeirechts, 4. Aufl., S. 994; Kutscha/Roggan, Große Lauschangriffe im Polizeirecht in Roggan (Hrsg.) Lauschen im Rechtsstaat, Gs Lisken, 2004, Seite 32 ff.

[97] s. hierzu auch Unabhängiges Landesamt für den Datenschutz Schleswig-Holstein, Stellungnahme zur Novellierung des HessSOG im Innenausschuss des Hessischen Landtages, Ausschußvorlage INA 17/3 Teil 1 Nr. 10.

§ 23 PolDVG gestattet die Rasterfahndung „zur Verhütung von Straftaten erheblicher Bedeutung“. Die Verhütung von Straftaten ist ein präventivpolizeilicher Zweck.

Allerdings ergibt sich aus der Definition der „Straftaten von erheblicher Bedeutung“ in § 1 Abs. 4 PolDVG, daß damit nicht nur schwerwiegende Straftaten, sondern auch Bagatelldelikte erfaßt sind. Hier nimmt § 23 Abs. 1 Ziff. 1 und 2 PolDVG aber eine weitergehende Einschränkung vor, so daß hier tatsächlich nur schwerwiegende Straftaten erfaßt sind. Damit ist der Anforderung des Bundesverfassungsgerichtes genügt, daß die Rasterfahndung nur zum Schutz hochrangiger Verfassungsgüter zulässig ist[98].

Das Bundesverfassungsgericht charaktersiert die Rasterfahndung als einen besonders intensiven Eingriff wegen der Möglichkeit zu Persönlichkeitsbildern, wegen der möglichen weiteren Folgen für Betroffene und wegen der großen Streubreite des verdachtslosen Eingriffs in das informationelle Selbstbestimmungsrecht. Daher ist die Rasterfahndung nur zulässig bei einer hinreichend konkreten Gefahr für hochrangige Rechtsgüter, und zwar einer gegenwärtigen oder konkreten Gefahr, denn derart intensive Grundrechtseingriffe darf der Gesetzgeber erst ab einer bestimmten Verdachts- oder Gefahrenstufe anordnen. Im Vorfeld der Gefahrenabwehr scheidet diese Maßnahme aus, sie darf nur „ultima ratio“ sein, wenn andere Maßnahmen ausgeschöpft sind.[99]

Diese Eingrenzungen enthält § 23 PolDVG nicht - die Regelung ist daher in der geltenden Form verfassungswidrig. § 23 PolDVG ermöglicht schon weit im Vorfeld einer konkreten Gefahr intensive Grundrechtseingriffe. Sie läßt ausreichend sein „wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass dies zur Verhütung dieser Straftaten erforderlich ist“. Derart vage Tatsachen reichen ebensowenig wie eine „allgemeine Bedrohungslage“ für die Rasterfahndung [100], also auch nicht die abstrakte Möglichkeit drohender Straftaten. Es fehlt jede Bezugnahme auf eine konkrete Gefahr für die in Abs. 1 genannten hochrangigen Rechtsgüter. Weiter fehlt eine Bestimmung, daß Rasterfahndung nur zulässig sein darf, wenn die Gefahrenabwehr „auf andere Weise nicht möglich ist“.

Damit ist § 23 PolDVG verfassungswidrig[101].

Bei einer Neuregelung ist zu prüfen, ob die präventivpolizeiliche Rasterfahndung überhaupt erforderlich ist. Bei schwerwiegenden Straftaten (und konkreten Verdachtsmomenten, also einer konkret bestehenden Gefahr) reicht das strafprozessuale Instrumentarium.

Rasterfahndung ist „kein besonders treffsicheres Instrument, vielleicht auch ein ziemlich schlechtes Fahndungs- und Vorbeugemittel“.[102] Es stellt sich die Frage, ob die präventive Rasterfahndung ein geeignetes Mittel zur Abwehr konkreter Gefahren ist.

---

[98] BVerfG, B. v. 04.04.2006 - 1 BvR 518/02
[99] ebd.
[100] ebd.
[101] so auch Brenneisen, Die präventiv-polieiliche Rasterfahndung im Lichte der aktuellen Rechtsprechung des BVerfG, DuD 2006, 685, 689.
[102] Brugger, Freiheit und Sicherheit, Baden-Baden 2004, S. 91

Eine Rasterfahndung bei konkreter Gefahr schwerer Straftaten ist immer doppelfunktional mit seltenem Schwerpunkt bei Gefahrenabwehr. Ein präventiver Schwerpunkt kann bei bestehendem Straftatverdacht nur bei einer situationsbedingt in den Vordergrund tretenden, gegenwärtigen Gefahr für ein höchstrangiges Rechtsgut gegeben sein.[103] Hinzu kommt die Problematik, daß bei Rasterfahndung das angenommene Täterprofil auf diskriminierenden Vorurteilen beruhen kann (diskriminierende Unterscheidungsmerkmale wie Migrationshintergrund, Religionszugehörigkeit, häufige Auslandsreisen, ausländische Kontaktpersonen etc.), sozial diskirminierende Wirkung haben[104] und zu unzulässigen Persönlichkeitsprofilen führen kann.

Präventive Rasterfahndung ist mehr ein Verdachtsgewinnungsinstrument als echte Gefahrenabwehr, es dient der Verdachtsaufklärung und der Gefahrerforschung[105] und wird auch als „spezifische Verdachtsschöpfungsmethode“ bezeichnet[106]. Für den vom Bundesverfassungsgericht für zulässig gehaltenen präventiven Einsatzbereich bei „konkreter Gefahr“ bleibt nur ein geringes Anwendungsfeld. Volkmann sagt daher zu Recht: „Die Rasterfahndung wird umso überflüssiger, je konkreter die Gefahr ist …. Die Rasterfahndung dürfte damit ein Fall für das Museum geworden sein…“[107]

3.7 Schußwaffengebrauch §§ 24 ff. hmbSOG

In § 25 Abs. 3 hmbSOG wurde der finale Todesschuß gesetzlich geregelt, und zwar sehr weitgehend nicht zur Abwehr einer *Lebensgefahr*, sondern auch zur Abwehr einer „unmittelbar bevorstehenden Gefahr einer schwerwiegenden Verletzung der körperlichen Unversehrtheit“.

Es fehlen empirische Daten, ob sich durch die Neuregelung der polizeiliche Schußwaffengebrauch verändert hat.

Gegen den finalen Todesschuss werden seit der Diskussion um den Musterentwurf für ein einheitliches Polizeigesetz in den 70er Jahren erhebliche Bedenken vorgebracht, weil das Todesstrafenverbot (Art. 102 GG) umgangen wird. Im Bereich der Gefahrenabwehr sind Prognoseunsicherheiten unvermeidlich sind. Ist die Tötung von Menschen schon nicht auf gesicherter Tatsachenbasis nach Abschluß eines Strafverfahrens zulässig, kann dies erst recht nicht auf ungesicherter Tatsachenbasis zulässig sein. In den polizeilichen Zwangslagen, die mit der Befugnis zum Todesschuß geregelt werden sollen, steht den Polizisten ohnehin das Notwehr- und Nothilferecht zur Seite. Die gesetzliche Erlaubnis könnte zum Absinken der Hemmschwelle führen[108].

Die Länder Schleswig-Holstein, Nordrhein-Westfalen und Mecklenburg-Vorpommern verzichten auf die gesetzliche Regelung des finalen Todesschusses.

---

[103] Knemeyer, Polizei- und Ordnungsrecht, 11. Aufl. München 2007, S. 63
[104] s. hierzu Achelpöhler/Niehaus, DÖV 2003, 50; Brenneisen, aaO. S. 688
[105] BVerfG, B. v. 04.04.2006 - 1 BvR 518/02; Anm. Volkmann, JZ 2006, 918;
[106] Brenneisen, Die präventiv-polizeiliche Rasterfahndung im Lichte der aktuellen Rechtsprechung des BVerfG, DuD. 2006, 685, 687
[107] JZ 2006, 918, 920
[108] vgl. Funk/Werkenthin, KJ 1976, 128; zur Problematik s. Lisken in Lisken/Denninger, Handbuch des Polizeirechtes, 3. Aufl. F 866 ff und Rachor in Lisken/Denninger, Handbuch des Polizeirechtes, 4. Aufl. F 990

Nach der Entscheidung des Bundesverfassungsgerichtes zum Luftsicherheitsgesetz[109] ist es dem Staat im Hinblick auf das Verhältnis von Lebensrecht und Menschenwürde untersagt, durch eigene Maßnahmen unter Verstoß gegen das Verbot der Mißachtung der menschlichen Würde in das Grundrecht auf Leben einzugreifen. Der Staat muß sich schützend und fördernd vor das Leben jedes Einzelnen stellen und es auch vor Angriffen Dritter bewahren. Danach dürfen von staatlichen Eingriffen Personen nicht betroffen werden, die auf die Herbeiführung der eigentlichen Gefahr keinen Einfluß genommen haben. Dies gilt selbst in Extremsituationen wie dem Fall des Luftsicherheitsgesetzes, in dem das Flugzeug, in dem die Drittbetroffenen sitzen, selbst als Angriffsmittel genutzt wird, in dem sie also bereits zum Objekt der Täter geworden sind. Genau in dieser Situation verbietet aber das Bundesverfassungsgericht dem Staat, diese Personen selbst noch zu Objekten der Rettungshandlung zum Schutze anderer zu machen, weil der Mensch damit mißachtet wird als Subjekt mit Würde und unveräußerlichen Rechten**.**

Jede Relativierung der Menschenwürde gefährdet die humanitäre freiheitliche Grundhaltung der Verfassung.

Das Bundesverfassungsgericht hat ausdrücklich die gesetzliche Ermächtigung zur Rechtfertigung solcher Eingriffe getrennt von der möglicherweise anderen strafrechtlichen Beurteilung der Beamten, die in einer solchen auswegslosen Situation Entscheidungen treffen müssen.

Andererseits hat das Bundesverfassungsgericht in der Entscheidung zum Luftsicherheitsgesetz tödlich wirkende Maßnahmen gegen den mutmaßlichen „Täter“ eines Flugzeugangriffs zum Lebensschutz ohne Gefährdung des Lebens Dritter für zulässig gehalten.

Der „finale Todesschuss“, wie er in § 25 I hmbSOG geregelt ist, verstößt daher nicht offenkundig gegen die Entscheidung des Bundesverfassungsgerichtes zum Luftsicherheitsgesetz. Er sollte dennoch im Hinblick auf das Todesstrafenverbot auf den Prüfstand. Beamte im Einsatz etwa bei Geiselnahmen benötigen keine gesetzliche Regelung, weil ihnen in der Notsituation zum Schutz von Leib und Leben der Geisel oder anderer unbeteiligter Dritter stets das Nothilferecht zur Seite steht, das zur Rechtfertigung und Schuldlosigkeit in strafrechtlicher Hinsicht führt.

Die Neuregelung 2005 wurde begründet „zum Schutz der vollziehenden Polizeibeamten vor schädlichen Bedenken über die etwaige Rechtswidrigkeit des tödlich wirkenden Schusses zur Lebensrettung“[110]. Genau hierfür sind aber die vorhandenen rechtlichen Instrumente Notwehr, Nothilfe und übergesetzlichem Notstand ausreichend. Eine gesetzliche Regelung des finalen Todesschusses ist ein weiterer Baustein in der Militarisierung der Polizei und kann - langfristig gesehen - zu einem Absinken der Eingriffsschwelle führen.

Auch hier ist anzuregen, empirische Daten zu erheben, um die Notwendigkeit der gesetzlichen Regelung und ggf. verändertes Einsatzverhalten zu prüfen.

---

[109] BVerfG vom 15. Februar 2006 - 1 BvR 357/05 -

[110] Begründung des Gesetzentwurfes vom 14.12.2004 - LT Drs. 18/1487

3.8 Taser § 14 Abs. 4 hmbSOG

Für diese neu eingeführte Waffe fehlt die Evaluierung.

In der Gesetzesbegründung wird das „Elektroimpulsgerät Advanced Taser“ als „reine Defensivwaffe“ und „Schock-Lähmungswaffe“ bezeichnet mit einem geringeren Risiko als bei dem Gebrauch anderer Schusswaffen. Es handele sich um eine „mildere Form des Schußwaffengebrauches“ lediglich mit der Gefahr von Verletzungen durch Stürze[111]. Die Einführung erfolgte auf Empfehlung der Innenministerkonferenz.

Gerade aus jüngerer Zeit sind wegen Todesfällen nach Tasergebrauch erhebliche Bedenken gegen diese Waffe vorgebracht worden:

Nach einem Bericht von amnesty international[112] ist es seit 2001 mindestens zu 277 Todesfällen gekommen. Selbst in offiziellen Studien im Auftrag des US-Justizministeriums wird eingestanden, dass der Taser eine Waffe ist, die Menschen verletzen und in manchen Fällen töten kann[113]. Der Taser wird auch von der deutschen Sektion Polizei von amnesty international kritisch gesehen, weil

- die Eingriffsschwelle gegenüber einer Schußwaffe absinkt im routinemäßigen Gebrauch bis hin zur Nutzung als Disziplinierungsinstrument[114]
- die Waffe erhebliche Schmerzen verursachen kann, ohne dass sichtbare Spuren der Fremdeinwirkung verbleiben, also das Folterverbot umgangen werden kann[115]
- die bekannt gewordenen Todesfälle eine Neubewertung der Waffe und ihres Nutzens erforderlich machen.

Vorliegende Studien basieren auf Tests mit gesunden Versuchspersonen, Todesfälle sind dagegen aufgetreten im Zusammenhang mit der typischen polizeilichen Klientel, etwa nach Drogengebrauch, bei gesundheitlichen Vorschäden, psychischen Erkrankungen und vor allem bei erheblichen Erregungszuständen. Spektakulär war der Tod eines polnischen Touristen mit Flugangst und ohne englische Sprachkenntnisse in 2007 in Vancouver/Kanada[116].

Ausreichende Untersuchungen zu Wirkungen der Waffe auf die Personenkreise, mit der die Polizei vermehrt zu tun hat, liegen nicht vor. Kanada hat Untersuchungen angeordnet. Amnesty International fordert unabhängige Untersuchungen. In Österreich wird der Taser-Einsatz zwischen Innen- und Justizministerium kontrovers diskutiert[117].

Die weltweiten Erfahrungen zeigen, dass die Werbeankündigungen der Hersteller sehr kritisch bewertet werden müssen.

Die Erkenntnis, dass die Einschätzung „nicht-tödliche Distanzwaffe“ nicht haltbar ist, muß zu einer Neubewertung der Waffe führen. Der Konflikt zwischen Menschenwür-

---

[111] Drs. 18/1487
[112] www.amnestyusa.org/document
[113] zitiert nach Spiegel-online vom 08.10.2007, Elektroschocker-Studie: Tausendmal getasert - drei im Krankenhaus www.spiegel.de/Wissenschaft/mensch/0,1518,510156,00.htm; so auch http://www.heise.de/tp/r4/artikel/22/22350/1.html
[114] spiegel-online vom 19.09.2007, www.spiegel.de/panorama/justiz/0,1518,506757,00.htm
[115] http://www.unog.ch/80256EDD006B9C2E/(httpNewsByYear_en)/D3DD9DE87B278A87C125739C0054A81C?OpenDocument
[116] http://www.heise.de/tp/r4/artikel/26/26618/1.html
[117] orf-online, zitiert nach http://de.wikipedia.org/wiki/Elektroschockpistole#cite_note-6

de (Folterverbot) und „Bequemlichkeit“ für Polizeibeamte sollte dazu führen, den Taser abzuschaffen oder nur für spezielle Sondereinsatzkommandos zuzulassen

- außerhalb des alltäglichen Polizeidienstes
- nur für extrem schwierige Lagen mit erheblicher Lebensgefahr, ausschließlich als alternative zum zulässigen Schußwaffengebrauch
- nicht gegen Versammlungen und Menschenmengen.

Eine solche Begrenzung der Anwendung müßte bereits die gesetzliche Regelung enthalten. Gegenwärtig ist die Anwendungsbegrenzung in Hamburg allein der Polizeipraxis überlassen, obwohl die Beschränkung auf das MEK Teil der Begründung bei der Einführung war.

In jedem Fall sollte die gesetzliche Ermächtigung um die Beschränkungen erweitert werden, daß Taser nur für speziell geschulte polizeiliche Sondereinheiten und nicht als reguläre Waffe Verwendung finden dürfen. Der Einsatz sollte weiter gesetzlich beschränkt werden ausschließlich als milderes Mittel bei zulässigem Schusswaffengebrauch bei erheblicher unmittelbarer Gefahr für Leib oder Leben.

3.9 Gewahrsamsdauer § 13 c hmbSOG

2005 wurde die höchstzulässige Dauer des Präventivgewahrsams mit richterlicher Anordnung in § 13 c hmgSOG erhöht auf bis zu 14 Tagen einerseits für den Gewahrsam zur Verhinderung von Straftaten (§ 13 Abs. 1 Ziff 2 hmbSOG), andererseits für die Durchsetzung des neu geschaffenen Betretungs- und Aufenthaltsverbotes nach § 12 b hmbSOG (§ 13 Abs. 1 Ziff 4 hmbSOG).

Nach den Gesetzgebungsmaterialien erfolgte die Erweiterung des Verhinderungsgewahrsams auf bis zu 14 Tage wegen der Fußball-Weltmeisterschaft. Dieser Zweck hat sich zwischenzeitlich erledigt. Zielgruppe sollte weiter sein der BTM-Straßenhandel, Stalking und Hooligans. Freiheitsentziehung darf von der Polizei nicht als „Ersatzbestrafung“[118] oder als Arbeitserleichterung mißbraucht werden. Es fehlen bislang belastbare Daten, ob sich die Verlängerung des Gewahrsams für Aufgaben der Gefahrenabwehr als notwendig erwiesen hat und wie oft der Langzeitgewahrsam angeordnet wurde.

Gegen die Gewahrsamsdauer von bis zu 14 Tagen bestanden bereits bei der Einführung verfassungsrechtliche Bedenken[119]. Zum einen ist wegen der Intensität des Eingriffs in die persönliche Freiheit ein längerfristiger Gewahrsam in der Regel unverhältnismäßig. Zum anderen ist die Prognose einer lang dauernden fortbestehenden Tatbereitschaft nicht durch äußere Tatsachen zu begründen, sondern beruht im hohen Maße auf Vermutungen und willkürlichen Prognosen. Schließlich steigt mit zunehmender Dauer der Freiheitsentziehung der repressive Charakter als Bestrafungs- und Abschreckungsinstrument, der präventive Charakter als Gefahrverhinderungsinstrument tritt in den Hintergrund. Dies gilt insbesondere in den Anwendungsfällen der Durchsetzung von Aufenthalts- und Betretungsverboten nach § 12 b Abs. 2

[118] BVerfG, B. v. 13.12.2005 - 2 BvR 447/05
[119] s.hierzu Merten/Merten, Hamburgisches Polizei- und Ordnungsrecht, Kommentar, 2007 zu § 13 c SOG Anm. 7 m.w.N

SOG, die selbst schon allein auf der Prognose beruhen, eine Person wolle an einem bestimmten Ort innerhalb der nächsten Zeit (bis zu 12 Monate) eine Straftat (welcher Art und Schwere auch immer) begehen.

Der Hauptanwendungsfall des Verhinderungsgewahrsams ist das Versammlungsrecht. Dies wird sich bei einer Überprüfung der Anwendungen in Hamburg erweisen. Gerade hier geht es häufig um Straftaten minderer Schwere oder mit besonderer Prognoseunsicherheit, denn es reicht oft schon schwarze Bekleidung oder ein Halstuch, um Gewalttaten oder Vermummungsabsichten zu unterstellen. Schon die in § 13 Abs. 1 Ziff. 2 genannten Indizien für eine bevorstehende Begehung einer Straftat oder Ordnungswidrigkeit von erheblicher Bedeutung lassen keinen sicheren Schluß auf die künftigen Absichten des Betroffenen zu: es reicht ein früheres Antreffen „in vergleichbarer Lage“ oder ein Dateieintrag und „Umstände“, nach denen die Wiederholung der Tat bevorsteht. Es ist weder eine besondere Schwere der Anlaßtat noch ein besonders erhärteter Tatverdacht oder Gefahrenverdacht erforderlich. Aus geringen äußeren Umständen wird auf unbekannte innere Umstände (Absicht der Wiederholung) geschlossen, die einer objektiven Tatsachenüberprüfung nicht zugänglich sind.

Bei einer Novellierung des Hamburger Polizeirechtes sollte überprüft werden, ob die Verlängerung der Dauer des Gewahrsams in § 13 c hmbSOG bis zu 14 Tage Freiheitsentziehung erforderlich ist und wie oft mehr als 2 Tage bisher richterlich angeordnet wurden. Bei dieser Gelegenheit sollte auch geklärt werden, wie viele polizeiliche Gewahrsamnahmen in den letzten Jahren überhaupt einer Richterentscheidung zugeführt wurden und wie viele ohne Richterbeteiligung erfolgten, sowie wie hoch die Quote der richterlichen Anordnung, der nachträglichen gerichtlichen Anfechtung und der Bestätigung der Polizeimaßnahmen durch die Gerichte ist. Es sollten auch Zahlen erhoben werden, wie viele polizeiliche Gewahrsamnahmen und richterliche Anordnungen im Zusammenhang mit Versammlungen, mit Fußballereignissen, mit Beschaffungskriminalität und Stalking erfolgten, und wie viele Freiheitsentziehungen gerichtlich angefochten wurden.

Nach zutreffender Ansicht ist Gewahrsam nur eine kurzfristige und vorläufige Maßnahme zur Abwehr einer unmittelbaren Gefahr[120]. Nur bei Beachtung der Kurzfristigkeit kann ein Konflikt mit der bundesrechtlichen Regelung des Haftgrundes der Wiederholungsgefahr in § 112 a StPO vermieden werden[121]. Danach ist die Untersuchungshaft, also Freiheitsentziehung, aus präventiven Gründen der Straftatenverhinderung nur zulässig bei dringendem Tatverdacht besonders schwerwiegender Delikte. Langzeitgewahrsam auf ungesicherter Prognose bei geringen Straftaten oder Ordnungswidrigkeiten ist ein Systemwiderspruch.

4 Empfehlungen

Die beiden Hamburger Polizeigesetze sollten einer gründlichen Revision unterzogen werden und in einem einheitlichen Hamburger Polizeigesetz zusammengefaßt werden. Die Speicherung und Verarbeitung von Daten und technische Überwachungs-

[120] Rachor in: Lisken/Denninger, Handbuch des Polizeirechtes, 4. Aufl 2007, Kap. F Anm. 631, 633 634
[121] Rachor, a.a.O. Anm. 633

maßnahmen sollten gegenüber den grundlegenden polizeilichen Eingriffsbefugnissen kein Eigenleben führen. Dies gilt insbesondere für heimliche informationstechnische Eingriffe.

Der zeitliche Abstand zum 09.11.2001 sollte es ermöglichen, die neuen Eingriffsbefugnisse auf ihre Notwendigkeit und Tauglichkeit zum angegebenen Zweck zu überprüfen. Die Erfahrungen mit allen neuen technischen Überwachungsbefugnissen sollten ausgewertet werden.

Die jüngere Rechtsprechung des Bundesverfassungsgerichtes zwingt zu mehr gesetzgeberischer Sorgfalt:

1. Präventive Polizeiaufgaben einerseits, repressive Aufgaben und Strafverfolgungsvorsorge andererseits sind wegen der verschiedenen Gesetzgebungskompetenzen sauber zu trennen.

2. Auch für die Befugnisse zu Datenerhebung, Datenverarbeitung und Zweckveränderung von gespeicherten Daten sollten präventive bzw. repressive Zwecke gesetzgeberisch auseinandergehalten werden.

3. Alle Befugnisse zu Überwachungsmaßnahmen mit technischen Mitteln sollten im Hinblick auf Normenbestimmtheit und Normenklarheit überarbeitet werden.

4. Der Kernbereichsschutz sollte für alle Überwachungsbefugnisse überarbeitet werden.

5. Videoüberwachung und automatischer Kfz-Kennzeichenabgleich sollten gestrichen werden.

6. Der Anwendungsbereich der Rasterfahndung für präventivpolizeiliche Zwecke unter Beachtung der Vorgaben des Bundesverfassungsgerichtes sollte überprüft werden, ggf. sollte auf die Rasterfahndung im präfentiven Polizeigesetz verzichtet werden.

7. Die Befugnisse zur Datenverarbeitung sollten überarbeitet, der Schutz der persönlichen Daten vor polizeilichen Persönlichkeitsprofilen sollte gestärkt werden. Zweckänderungen von Daten sollten restriktiv geregelt werden.

8. Die gesetzliche Regelung des finalen Todessschusses ist überflüssig und läßt ein Absinken der Handlungsschwelle befürchten.

9. Der Taser sollte wegen des Todes- und Mißbrauchsrisikos abgeschafft, hilfsweise auf die Verwendung durch besonders geschulte Sondereinheiten gesetzlich beschränkt werden.

10. Die Praxis des Präventivgewahrsams sollte überprüft werden. Die Dauer des Langzeitgewahrsams sollte für alle Anwendungsfälle auf 2 - 4 Tage beschränkt werden.