Ralph Glücksmann

Hamburgisches Gesetz über die Datenverarbeitung der Polizei

Kommentar, 1. Auflage 2005

Gesetz über die Datenverarbeitung der Polizei
vom 2. Mai 1991 (GVBl. S. 187, 191), zuletzt geändert am 6. Oktober 2005 (GVBl. S. 424)

Erster Abschnitt

Anwendungsbereich und allgemeine Befugnisse zur Datenerhebung

§ 1 Anwendungsbereich, Begriffsbestimmungen

(1) Dieses Gesetz findet Anwendung, soweit die Vollzugspolizei (Polizei) zur Erfüllung ihrer Aufgaben nach dem Gesetz zum Schutz der öffentlichen Sicherheit und Ordnung (SOG) vom 14. März 1966 (Hamburgisches Gesetz- und Verordnungsblatt Seite 77), zuletzt geändert am 2. Mai 1991 (Hamburgisches Gesetz- und Verordnungsblatt Seite 187), in der jeweils geltenden Fassung Daten verarbeitet. Zu den in Satz 1 genannten Aufgaben gehört auch die Erhebung und weitere Verarbeitung von Daten

1. **zur Verhütung von Straftaten und zur Vorsorge für die Verfolgung künftiger Straftaten (vorbeugende Bekämpfung von Straftaten) und**
2. **zur Vorbereitung für die Hilfeleistung und das Handeln in Gefahrenfällen.**

(2) Soweit dieses Gesetz keine besondere Regelung enthält, findet das Hamburgische Datenschutzgesetz vom 5. Juli 1990 (Hamburgisches Gesetz- und Verordnungsblatt Seiten 133, 165, 226) in der jeweils geltenden Fassung Anwendung.

(3) Polizei im Sinne dieses Gesetzes sind die für vollzugspolizeiliche Aufgaben, insbesondere die für unaufschiebbare Maßnahmen in allen Fällen der Gefahrenabwehr (§ 3 Absatz 2 Buchstabe a SOG) und die Verfolgung von Straftaten und Ordnungswidrigkeiten zuständigen Organisationseinheiten innerhalb der zuständigen Behörde.

(4) Straftaten von erheblicher Bedeutung sind

1. **Verbrechen,**
2. **Vergehen, die im Einzelfall nach Art und Schwere geeignet sind, den Rechtsfrieden besonders zu stören, soweit sie**
   a) sich gegen Leib, Leben oder Freiheit einer Person oder bedeutende Sach- oder Vermögenswerte richten,
   b) auf den Gebieten des unerlaubten Waffen- oder Betäubungsmittelverkehrs, der Geld- oder Wertzeichenfälschung, der Vorteilsannahme oder -gewährung, der Bestechlichkeit oder Bestechung (§§ 331 bis 335 des Strafgesetzbuches) oder des Staatsschutzes (§§ 74a und 120 des Gerichtsverfassungsgesetzes)begangen werden,
   c) gewerbs-, gewohnheits-, serien-, bandenmäßig oder sonst organisiert begangen werden.

(5) Abwehr einer Gefahr im Sinne dieses Gesetzes ist auch die Beseitigung einer Störung der öffentlichen Sicherheit oder Ordnung.

(6) Kontakt- oder Begleitpersonen im Sinne dieses Gesetzes sind Personen, die mit einer Person, von der tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass diese Person Straftaten begehen wird, in einer Weise in Verbindung stehen, die die Erhebung ihrer personenbezogenen Daten zur vorbeugenden Bekämpfung dieser Straftaten erfordert.

(7) Organisierte Kriminalität im Sinne dieses Gesetzes ist die von Gewinn- oder Machtstreben bestimmte planmäßige Begehung von Straftaten nach Absatz 4, wenn mehr als zwei Beteiligte auf längere oder unbestimmte Dauer arbeitsteilig

1. **unter Verwendung gewerblicher oder geschäftsähnlicher Strukturen,**
2. **unter Anwendung von Gewalt oder anderer zur Einschüchterung geeigneter Mittel oder**
3. **unter Einflussnahme auf Politik, Medien, öffentliche Verwaltung, Justiz oder Wirtschaft**

zusammenwirken.

1

Absatz 1 umschreibt den Anwendungsbereich dieses Gesetzes. Es umfaßt das gesamte gefahrenabwehrende Handeln der Polizei. Die Umschreibung des Anwendungsbereiches erlaubt ohne eine entsprechende Befugnisnorm keine Eingriffe in Rechte der Bürger. Allerdings darf die Polizei aufgrund der Aufgabenzuweisung sogenannte schlicht-hoheitliche Handlungen vornehmen, die keine Eingriffe in Grundrechte enthalten, wie z.B. Streifengänge und -fahrten oder die polizeiliche Präsenz bei besonderen Anlässen oder an besonders gefährdeten Objekten. Satz 2 dient der Klarstellung. Damit wird verdeutlicht, daß die Polizei im Rahmen ihrer Zuständigkeit zur Gefahrenabwehr auch Straftaten zu verhüten und für die Verfolgung künftiger Straftaten vorzusorgen hat. Zugleich definiert diese Bestimmung den beide Aufgabenbestandteile zusammenfassenden Begriff „vorbeugende Bekämpfung von Straftaten“. Diese Aufgabe wird in unterschiedlicher Form wahrgenommen, z.B. durch Erhebung und Sammlung von Informationen über Personen, bei denen zu erwarten ist, daß sie künftig Straftaten begehen werden, durch die Analyse struktureller Zusammenhänge einer "kriminellen Szene", aber auch durch kriminalpolizeiliche Beratungsprogramme. Soweit mit diesen Maßnahmen in Rechte einzelner Bürger eingegriffen wird, bedarf es gesetzlicher Ermächtigungen. Als weiterer Teilaspekt der Gefahrenabwehr wird ferner die Aufgabe der Polizei genannt, sich auf die Hilfeleistung und Handeln in Gefahrenfällen vorzubereiten. Hierin liegt keine Verlagerung von Aufgaben anderer Behörden auf die Polizei. Vielmehr kann sie - insbesondere im Rahmen ihrer Eilzuständigkeit - Gefahren nur dann wirksam begegnen, wenn sie hierauf vorbereitet ist. Ferner gehören, ohne daß dies besonderer Erwähnung bedarf, zum Anwendungsbereich dieses Gesetzes auch die im HmbSOG nicht ausdrücklich geregelten Maßnahmen der Polizei zum Schutz privater Rechte sowie bei der Leistung von Vollzugshilfe für andere Behörden, die zu den „klassischen“ vollzugspolizeilichen Aufgaben gerechnet werden.

2

Absatz 2 stellt klar, daß neben den bereichsspezifischen Regelungen dieses Gesetzes die allgemeinen Bestimmungen des Hamburgischen Datenschutzgesetzes anzuwenden sind. Hierzu gehören insbesondere die im Hamburgischen Datenschutzgesetz enthaltenen Begriffsbestimmungen, die Verpflichtung, organisatorische und technische Maßnahmen zur Datensicherung zu treffen, sowie die Regelungen über die Schadensersatzpflicht, die Datenverarbeitung zu Forschungs- und Planungszwecken und über die Kontrollbefugnisse des Hamburgischen Datenschutzbeauftragten. Keiner besonderen Erwähnung in diesem

Zusammenhang bedarf, daß daneben selbstverständlich auch die allgemeinen Vorschriften des HmbSOG - insbesondere der „Störerbegriff“ und der Grundsatz der Verhältnismäßigkeit - bei Maßnahmen nach diesem Gesetz zu beachten sind.

3

Absatz 3 enthält eine Legaldefinition des Begriffs „Polizei“. Diese Definition orientiert sich am überkommenen Begriff der Vollzugspolizei, der auch im HmbSOG sowie im Hamburgischen Beamtengesetz (Abschnitt VII) Verwendung findet. Eine exaktere Abgrenzung ist aufgrund der Hamburger Verwaltungsstruktur nicht möglich, da innerhalb des Amtes Polizei auch andere Aufgaben erfüllt werden, die nicht vollzugspolizeilicher Natur sind. Insbesondere handelt es sich dabei um Funktionsbereiche, die - wie andere Verwaltungsbehörden - als Genehmigungs- und Überwachungsbehörden tätig werden. Nach dem hier gewählten funktionellen Polizeibegriff sind die letztgenannten Funktionsbereiche somit auch nicht Polizei im Sinne dieses Gesetzes. Die Datenverarbeitung in diesen Bereichen bestimmt sich ausschließlich nach den für diese Funktionsbereiche maßgeblichen Rechtsvorschriften (z.B. Straßenverkehrsgesetz) in Verbindung mit den einschlägigen Querschnittsgesetzen (insbesondere Verwaltungsverfahrensgesetz und Datenschutzgesetz). Durch diese Begriffsbestimmung wird zugleich deutlich, daß die Erfüllung der diesen Verwaltungsbereichen obliegenden Aufgaben kein polizeilicher Zweck im Sinne dieses Gesetzes darstellt. Die Nutzung (vollzugs-)polizeilicher Daten für Zwecke dieser Funktionsbereiche ist daher nach § 18 Absatz 1 Satz 2 nur unter den Voraussetzungen einer Datenübermittlung zulässig.

4

In Absatz 4 wird festgelegt, bei welchen Straftaten es sich um solche von erheblicher Bedeutung handelt. Diesem Begriff kommt eine zentrale Bedeutung zu, da er die Voraussetzung für bestimmte polizeiliche Maßnahmen, insbesondere für den Einsatz verdeckter Mittel zur Datenerhebung, darstellt. Ein geschlossener Straftatenkatalog, der die relevanten Straftatbestände enumerativ und abschließend auflistet, ist im Hinblick auf die Zielsetzung ungeeignet. Die Polizei soll durch den Einsatz verdeckter Maßnahmen in die Lage versetzt werden, Straftaten vorbeugend zu bekämpfen, die den Rechtsfrieden empfindlich stören. Neue Erscheinungsformen oder besondere Ausprägungen der Kriminalität etwa im Bereich des politisch oder religiös motivierten Extremismus oder unter Nutzung der neuen Kommunikationstechnologien haben dazu geführt, dass die Polizei trotz einer erheblichen Beeinträchtigung des Rechtsfriedens geeignete Überwachungsmaßnahmen nicht einsetzen konnte, weil die entsprechenden Tatbestände nicht im Katalog der Straftaten von erheblicher Bedeutung enthalten waren. Um auf neue, teilweise noch nicht vorhersehbare Herausforderungen der inneren Sicherheit und dementsprechend auch auf neue Straftatbestände reagieren zu können, wurde anstelle der Katalogtaten ein offener Straftatenkatalog gewählt. Nach Nummer 1 gelten alle Verbrechen als Straftaten von erheblicher Bedeutung. Diese Gewichtung ist sachgerecht, da Verbrechen generell erhebliche Schäden für andere Rechtsgüter zur Folge haben und insofern auch abwehrende polizeiliche Eingriffe von höherer Intensität rechtfertigen. Bei künftigen strafgesetzlichen Änderungen im Bereich der Verbrechenstatbestände sind keine weiteren Anpassungen in diesem Gesetz erforderlich. In Nummer 2 werden Vergehen erfasst, soweit sie im Einzelfall nach Art und Schwere geeignet sind, den Rechtsfrieden besonders zu stören, und einer der Fallgruppen der Buchstaben a) bis c) angehören. Die Straftatbestände werden dabei nach ihrem Schutzgut, nach

bestimmten Deliktsgruppen oder nach der Begehungsweise bestimmt. Straftaten sind danach geeignet, den Rechtsfrieden besonders zu stören, wenn sie sich gegen besonders bedeutsame Rechtsgüter richten oder aber auf Grund ihrer Deliktszugehörigkeit bzw. der Art und Weise der Tatausführung eine besondere Sozialschädlichkeit besitzen. Neben den Staatsschutzdelikten werden auch die Delikte der Vorteilsannahme und Bestechlichkeit erfasst. Die Bekämpfung der Korruption ist eine zentrale gesellschaftspolitische Aufgabe der Gegenwart. Das kollusive, von verwerflichem Gewinnstreben bestimmte Zusammenwirken von Amtsträgern und Personen in der Wirtschaft erschüttert in besonders hohem Maße das Vertrauen der Rechtsgemeinschaft in die Integrität der öffentlichen Verwaltung und verursacht hohen volkswirtschaftlichen Schaden. Die Möglichkeit, in diesem Deliktsbereich verdeckte Maßnahmen einzusetzen, ist für die vorbeugende Bekämpfung der Korruption von besonderer Bedeutung. Die getroffene Beschreibung der Straftatbestände trägt dem jeweiligen Gewicht des abzuwehrenden Angriffs und der Intensität des polizeilichen Eingriffs damit in der gebotenen Weise Rechnung und wahrt den Verhältnismäßigkeitsgrundsatz als rechtsstaatliche Generalschranke jeder staatlichen Maßnahme (vgl. zu einer vergleichbaren Regelung im Polizeigesetz des Freistaates Sachsen die Entscheidung des Verfassungsgerichtshofs des Freistaates Sachsen vom 14. Mai 1996 - Vf. 44-II-94 Rdnr. 232 ff -).

5

Die Klarstellung in Absatz 5 hinsichtlich des Begriffs „Abwehr einer Gefahr“ ist geboten, da im HmbSOG - anders als in den vergleichbaren Bestimmungen anderer Länder - die Beseitigung einer eingetretenen Störung jeweils ausdrücklich neben der Abwehr einer bevorstehenden bzw. unmittelbar bevorstehenden Gefahr genannt wird. Hieraus könnten sich Zweifel ergeben, ob in den Vorschriften, in denen als Tatbestandsvoraussetzung die Abwehr einer bevorstehenden bzw. unmittelbar bevorstehenden Gefahr genannt wird, auch die Beseitigung bereits eingetretener Störungen erfaßt sein soll. Keiner besonderen Erwähnung im Gesetz bedarf dagegen, daß zur Abwehr einer bevorstehenden Gefahr auch die Feststellung von Gefahrensituationen gehört, wenn Anhaltspunkte für die Entwicklung einer Gefahr gegeben sind.

6

In Absatz 6 wird der Begriff "Kontakt- oder Begleitperson" definiert, der in verschiedenen Bestimmungen dieses Gesetzes verwendet wird (vgl. § 6 Nummer 7, § 9 und § 16 Absatz 3). Erforderlich ist mehr als ein nur flüchtiger sozialer Kontakt. Es muß sich also um eine Person handeln, die mit einem potentiellen Straftäter in einer Weise in Verbindung steht, die erwarten läßt, daß durch diese Datenerhebung wichtige Hinweise gewonnen werden können. Diese Bestimmung betrifft somit insbesondere Personen, die enge persönliche oder geschäftliche Kontakte zu einem potentiellen Straftäter unterhalten oder die bei einem konkreten Anlaß eine solche Person begleiten.

§ 2 Grundsätze der Datenerhebung

(1) Die Polizei darf personenbezogene Daten nur erheben, soweit dies durch dieses Gesetz zugelassen ist. Anderweitige besondere Rechtsvorschriften über die Datenerhebung bleiben unberührt.

(2) Personenbezogene Daten sollen bei dem Betroffenen erhoben werden. Ohne dessen Kenntnis dürfen sie bei anderen öffentlichen und nicht-öffentlichen Stellen erhoben werden, wenn die Erhebung beim Betroffenen

1. nicht oder nicht rechtzeitig möglich ist,
2. nur mit unverhältnismäßig hohem Aufwand möglich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen des Betroffenen beeinträchtigt werden, oder
3. die Erfüllung der Aufgaben gefährden würde.

(3) Personenbezogene Daten sollen offen erhoben werden. Eine Datenerhebung, die nicht als polizeiliche Maßnahme erkennbar ist, ist zulässig, wenn durch anderes Handeln die Erfüllung einer bestimmten polizeilichen Aufgabe erheblich erschwert oder gefährdet würde und die Maßnahme nicht gezielt verdeckt wird. Eine Datenerhebung, die nicht als polizeiliche Maßnahme erkennbar sein soll (verdeckte Datenerhebung), ist außer in den in diesem Gesetz ausdrücklich zugelassenen Fällen nur zulässig, wenn die Erfüllung einer bestimmten polizeilichen Aufgabe bei anderem Handeln aussichtslos wäre oder wenn dies den überwiegenden Interessen des Betroffenen entspricht.

(4) Werden personenbezogene Daten beim Betroffenen oder bei Dritten erhoben, sind diese in geeigneter Weise hinzuweisen auf

1. die Rechtsgrundlage der Datenerhebung,
2. eine im Einzelfall bestehende Auskunftspflicht oder die Freiwilligkeit der Auskunft und
3. die beabsichtigte Verwendung der Daten.

Dieser Hinweis kann unterbleiben, wenn er wegen der besonderen Umstände offenkundig nicht erforderlich ist oder wenn hierdurch die Erfüllung der polizeilichen Aufgabe oder die schutzwürdigen Belange Dritter beeinträchtigt oder gefährdet würden.

1

Absatz 1 trägt dem Grundsatz Rechnung, daß die Erhebung personenbezogener Daten als Grundrechtseingriff zu bewerten ist und daher einem Gesetzesvorbehalt unterliegt. Die Polizei darf somit zum Zwecke der Gefahrenabwehr personenbezogene Daten nur erheben, wenn sie sich auf eine entsprechende Befugnisnorm stützen kann. Anderweitige Rechtsvorschriften im Sinne von Absatz 1 Satz 2 sind z.B. die Befugnis zur Datenerhebung nach der Strafprozeßordnung oder zur Führerscheinkontrolle nach § 4 Absatz 2 StVZO.

2

Die Absätze 2 und 3 normieren den Grundsatz, Daten offen und beim Betroffenen zu erheben. Er ergibt sich aus der Forderung des Bundesverfassungsgerichts, daß der Einzelne grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen soll. Datenerhebung beim Betroffenen ist insbesondere dessen Befragung, aber auch andere Formen der polizeilichen Wahrnehmung (z.B. die Beobachtung einer Person oder das Mithören von

Gesprächen). Abweichungen von diesem Grundsatz sind insbesondere die Einholung von Auskünften bei öffentlichen Stellen oder bei Dritten (Zeugen oder Auskunftspersonen) sowie die Auswertung allgemein zugänglicher Quellen. Diese Formen der Datenerhebung sind unter den Voraussetzungen von Absatz 2 Satz 2 zulässig. Satz 2 Nummer 1 betrifft insbesondere Fälle, in denen eine Befragung des Betroffenen nicht oder nur mit erheblicher zeitlicher Verzögerung möglich ist. Satz 2 Nummer 2 bezieht sich demgegenüber auf Fälle, in denen der Betroffene zwar innerhalb der zur Verfügung stehenden Zeit erreichbar wäre, die Befragung jedoch nur mit erheblichem Aufwand möglich ist. Dabei dürfen jedoch keine schutzwürdigen Interessen des Betroffenen beinträchtigt werden. Dies betrifft z.B. Fälle, in denen Dritte durch die Befragung von einem bestimmten Sachverhalt Kenntnis erlangen. Eine Gefährdung der Aufgabenerfüllung im Sinne von Satz 2 Nummer 3 wird insbesondere anzunehmen sein, wenn der Betroffene durch die Befragung Gelegenheit erhält, einen bestimmten Sachverhalt zu verschleiern.

3

Eine verdeckte Datenerhebung, die nur unter den eingeschränkten Voraussetzungen des Absatzes 3 Satz 2 zulässig ist, setzt begrifflich voraus, daß die Zugehörigkeit zur Polizei bewußt verschleiert wird. Ein verdecktes Vorgehen im Sinne dieser Bestimmung liegt somit noch nicht vor, wenn Polizeibeamte, die ihren Dienst in Zivilkleidung verrichten oder ein äußerlich nicht als solches zu erkennendes Dienstfahrzeug benutzen, wegen der besonderen Umstände des Einzelfalles vor einer Datenerhebung nicht ausdrücklich auf die Zugehörigkeit zur Polizei hinweisen. Diese Form der Datenerhebung ist unter den Voraussetzungen des Absatzes 3 Satz 2 zulässig. Erforderlich ist also, daß die Wahrnehmung eines bestimmten Sachverhaltes bei sofortiger Offenbarung wesentlich erschwert oder gefährdet würde. Nicht mehr unter die Voraussetzungen des Absatzes 3 Satz 2, sondern des Absatzes 3 Satz 3 fällt dagegen eine Datenerhebung, bei der die Zugehörigkeit zur Polizei bewußt verheimlicht wird oder bei der der Beamte unter einem Vorwand tätig wird. Die Erfüllung einer bestimmten polizeilichen Aufgabe ist dann aussichtslos, wenn nach den Umständen anzunehmen ist, daß bei einer offenen Befragung die erforderlichen Auskünfte nicht oder mit hoher Wahrscheinlichkeit nicht zu erlangen sind. Darüber hinaus ist eine verdeckte Datenerhebung dann zulässig, wenn dies den überwiegenden Interessen des Betroffenen entspricht, wenn also z.B. durch eine erkennbare polizeiliche Maßnahme ein Vorgang zusätzliche Publizität erlangt. Diese Regelung hat somit die gleiche Zielrichtung wie Absatz 2 Nummer 2. Soweit die verdeckte Datenerhebung von den Begriffsbestimmungen der §§ 9 ff erfaßt wird, bestimmen sich die Voraussetzungen und das Verfahren der Datenerhebung ausschließlich nach diesen Bestimmungen. Die hier vorgenommene Abgrenzung zwischen der offenen und verdeckten Datenerhebung entspricht auch der Bedeutung des Rechts auf informationelle Selbstbestimmung. In die Befugnis des einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden - also zu wissen, wer was wann und bei welcher Gelegenheit über eine Person weiß -, wird dann nicht besonders intensiv eingegriffen, wenn sich die Datenerhebung auf Wahrnehmungen in der „Sozialsphäre“ - also Verhaltensweisen oder Äußerungen in der Öffentlichkeit - bezieht, die auch jeder Privatperson ohne weiteres zugänglich wäre. Insofern ist es auch nicht geboten, diese Form der Datenerhebung von besonders hohen Anforderungen abhängig zu machen.

4

Befragte Personen sind nach Absatz 4 grundsätzlich auf die Rechtsgrundlage der Datenerhebung, über die Auskunftspflicht oder Freiwilligkeit einer Auskunft sowie die beabsichtigte Verwendung der Daten zu unterrichten. Auf den Hinweis kann unter den Voraussetzungen des Satzes 2 verzichtet werden. Hierzu gehören insbesondere Situationen, in denen sich der Grund der Datenerhebung bereits aus den Umständen der Befragung ergibt.

§ 3 Befragung und Auskunftspflicht
(1) Die Polizei darf jede Person befragen, wenn auf Grund tatsächlicher Anhaltspunkte anzunehmen ist, dass sie sachdienliche Angaben machen kann, die für die Erfüllung einer bestimmten polizeilichen Aufgabe erforderlich sind. Für die Dauer der Befragung dürfen diese Personen angehalten werden.
(2) Eine Person, deren Befragung nach Absatz 1 zulässig ist, ist verpflichtet, auf Frage ihren Namen, Vornamen, Tag und Ort der Geburt, Wohnanschrift und Staatsangehörigkeit anzugeben. Sie ist zu weiteren Auskünften nur verpflichtet, soweit gesetzliche Handlungspflichten bestehen oder Tatsachen die Annahme rechtfertigen, dass sie sachdienliche Angaben zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes, für Leib, Leben oder Freiheit einer Person oder für bedeutende Sach- oder Vermögenswerte machen kann. Eingriffe in das Fernmeldegeheimnis (Artikel 10 Grundgesetz) sind nur unter den Voraussetzungen der §§ 10a bis 10c zulässig.
(3) §§ 52 bis 55 und § 136a der Strafprozessordnung gelten entsprechend.

1

Das dieser Vorschrift zugrundeliegende Auskunftsrecht der Polizei wurde früher aus der polizeilichen Generalklausel abgeleitet. Die Befragung kann sich auf alle Angaben beziehen, die für die Erfüllung einer bestimmten polizeilichen Aufgabe erforderlich sind. Soweit mit der Befragung die Erhebung personenbezogener Daten verbunden ist, hat sich diese nach den weiteren Vorschriften dieses Gesetzes zu richten (insbesondere §§ 4 und 6). Das Anhalten nach Absatz 1 Satz 2 bewirkt allenfalls eine kurzfristige Freiheitsbeschränkung, die keiner vorherigen Entscheidung durch einen Richter nach Artikel 104 des Grundgesetzes bedarf.

2

Gemäß Absatz 2 Satz 1 ist eine Person bei einer Befragung durch die Polizei lediglich verpflichtet, ihren Namen, Vornamen, Tag und Ort der Geburt, Wohnanschrift und Staatsangehörigkeit anzugeben. Verstöße hiergegen können nach § 111 des Gesetzes über Ordnungswidrigkeiten geahndet werden. Weitere Auskünfte kann die Polizei nur verlangen, wenn eine gesetzliche Handlungspflicht des Betroffenen besteht. Insbesondere im Zusammenhang mit der Durchführung der Rasterfahndung nach den Anschlägen in New York vom 11. September 2001 hat sich jedoch gezeigt, dass die bestehenden Regelungen zu unbestimmt sind und daher der Klarstellung bedürfen. So wurde bei weiteren Überprüfungen des gerasterten Personenkreises in Hamburg deutlich, dass durch Auskünfte unter anderem über Finanztransaktionen wichtige Erkenntnisse über die Strukturen des

Terrornetzes und noch unentdeckte Terroristen gewonnen werden könnten. Aus diesem Grund nahmen die Ermittler auch Befragungen auf der Grundlage allgemeiner polizeilicher Datenerhebungsnormen bei der Schufa und bei Finanzinstituten vor. Ziel dieser Befragungen war die Übermittlung von Kontobewegungen an die Polizei Hamburg. Bei den befragten Personen und Institutionen handelt es sich stets um sog. Nichtstörer, die gemäß § 10 HmbSOG nur in Fällen einer unmittelbar bevorstehenden Gefahr zur Auskunft verpflichtet sind. Das Verwaltungsgericht Hamburg hat in seiner Eilentscheidung vom 27. Februar 2002 (14 VG 446/2002) zur Rasterfahndung zwar bestätigt, dass nach den Anschlägen vom 11. September 2001 von einer „unmittelbar bevorstehenden Gefahr“ auszugehen war. Dabei hat das Gericht in besonderer Weise auf den engen zeitlichen Zusammenhang zwischen den Anschlägen und der Anordnung der Rasterfahndung abgestellt. Durch schlichten Zeitablauf wird dieser enge Zusammenhang fortwährend gelockert. Aus diesem Grund enthält Absatz 2 Satz 2 eine grundsätzliche Auskunftspflicht, falls eine Person sachdienliche Angaben zur Abwehr einer Gefahr für überragende Rechtsgüter machen kann. Mit der in Absatz 3 enthaltenen Verweisung auf bestimmte Vorschriften der Strafprozeßordnung wird sichergestellt, daß die dort normierten Aussage- und Zeugnisverweigerungsrechte sowie das Verbot bestimmter Vernehmungsmethoden auch hier Anwendung finden.

§ 4 Identitätsfeststellung und Prüfung von Berechtigungsscheinen
(1) Die Polizei darf die Identität einer Person feststellen,
1. soweit es im Einzelfall erforderlich ist zur Abwehr einer bevorstehenden Gefahr oder einer Aufgabe der Amts- oder Vollzugshilfe,
2. wenn sie an einem Ort angetroffen wird, von dem Tatsachen die Annahme rechtfertigen, dass dort
a) Personen Straftaten von erheblicher Bedeutung verabreden, vorbereiten oder verüben,
b) sich Personen aufhalten, die gegen aufenthaltsrechtliche Strafvorschriften verstoßen,
c) sich gesuchte Straftäter verbergen,
3. wenn sie in einer Verkehrs- oder Versorgungsanlage oder -einrichtung, einem öffentlichen Verkehrsmittel, Amtsgebäude oder in einem besonders gefährdeten Objekt oder in dessen unmittelbarer Nähe angetroffen wird und Tatsachen die Annahme rechtfertigen, dass in oder an diesem Objekt Straftaten begangen werden sollen, durch die Personen oder das Objekt erheblich gefährdet sind,
4. an einer Kontrollstelle, die von der Polizei eingerichtet worden ist, um eine Straftat nach § 129a des Strafgesetzbuchs, eine der in dieser Vorschrift bezeichneten Straftaten oder eine Straftat nach § 250 Absatz 1 Nummer 1 oder 2, nach § 255 des Strafgesetzbuchs in den vorgenannten Begehungsformen oder nach § 27 Absatz 1 und Absatz 2 Nummer 3 Buchstabe a des Versammlungsgesetzes vom 15. November 1978 mit der Änderung vom 9. Juni 1989 (Bundesgesetzblatt I 1978 Seite 1790, 1989 Seite 1059) zu verhüten, soweit auf Grund tatsächlicher Anhaltspunkte anzunehmen ist, dass solche Straftaten begangen werden sollen.
(2) Die Polizei darf im öffentlichen Raum in einem bestimmten Gebiet Personen kurzfristig anhalten, befragen, ihre Identität feststellen und mitgeführte Sachen in Augenschein nehmen, soweit auf Grund von konkreten Lageerkenntnissen anzunehmen ist, dass in diesem Gebiet Straftaten von erheblicher Bedeutung

begangen werden und die Maßnahme zur vorbeugenden Bekämpfung der Straftaten erforderlich ist.
(3) Zur Feststellung der Identität dürfen Namen, frühere Namen, Vornamen, Geburtsdatum, Geburtsort, Geschlecht, Staatsangehörigkeit und Anschrift erhoben werden.
(4) Zur Feststellung der Identität darf die Polizei die erforderlichen Maßnahmen treffen. Sie darf
1. den Betroffenen anhalten,
2. den Betroffenen oder Auskunftspersonen nach seiner Identität befragen,
3. verlangen, dass der Betroffene mitgeführte Ausweispapiere zur Prüfung aushändigt,
4. den Betroffenen festhalten,
5. den Betroffenen und die von ihm mitgeführten Sachen nach Gegenständen durchsuchen, die zur Identitätsfeststellung dienen können,
6. den Betroffenen zur Dienststelle bringen,
7. In den Fällen des Absatzes 1 unter den Voraussetzungen des § 7 erkennungsdienstliche Maßnahmen durchführen.
Maßnahmen nach den Nummern 4 bis 6 dürfen nur getroffen werden, wenn die Identität auf andere Weise nicht oder nur unter erheblichen Schwierigkeiten festgestellt werden kann oder wenn tatsächliche Anhaltspunkte dafür bestehen, dass Angaben unrichtig sind.
(5) Die Polizei darf verlangen, dass ein Berechtigungsschein zur Prüfung ausgehändigt wird, wenn der Betroffene auf Grund einer Rechtsvorschrift oder einer vollziehbaren Auflage in einem Erlaubnisbescheid verpflichtet ist, diesen Berechtigungsschein mitzuführen.

1

Eine Befugnis zur Personalienfeststellung ist bereits in § 12 Absatz 1 HmbSOG enthalten. Diese Bestimmung ist allerdings zu unbestimmt, um modernen verfassungsrechtlichen Anforderungen genügen zu können. Mit dieser Vorschrift wird daher eine spezielle Norm für Identitätsfeststellungen durch die Polizei geschaffen. Zweck der Identitätsfeststellung ist entweder, die Personalien einer unbekannten Person festzustellen, oder zu prüfen, ob diese mit einer gesuchten Person identisch ist. Die Befugnis nach Absatz 1 Nummer 1 1. Alternative setzt eine bevorstehende Gefahr voraus. Die Polizei darf also nicht willkürlich Personen zur Feststellung ihrer Identität überprüfen. Hierunter fällt auch die Identitätsfeststellung zur Sicherung zivilrechtlicher Ansprüche, soweit dies Aufgabe der Polizei ist. Die Befugnis zur Identitätsfeststellung nach Absatz 1 Nummer 1 3. Alternative soll der Polizei z.B. ermöglichen, anläßlich der Gewährung von Amts- oder Vollzugshilfe zugunsten einer anderen Behörde den richtigen Adressaten für ihr Vorgehen festzustellen.

2

Absatz 1 Nummer 2 stellt die Rechtsgrundlage für die sogenannte Razzia dar, bei der unter den genannten Voraussetzungen ein konkreter Verdacht gegen die zu überprüfenden Personen nicht erforderlich ist. Vielmehr werden alle Personen an solchen Orten, die nicht offensichtlich keine Beziehung zu den Anlaßtätigkeiten haben, von der Feststellungsbefugnis erfaßt. Die Regelung unterscheidet nicht zwischen Störern und Nichtstörern. Sie bewirkt eine reine Ortshaftung. Grundsätzlich kann jeder, der an einem solchen Ort anwesend ist, ereignisunabhängig - auch

routinemäßig - polizeilich überprüft werden. Die Maßnahme trägt dem Umstand Rechnung, daß es im Interesse einer wirksamen Gefahrenabwehr im Vorfeld konkreter Eingriffsmaßnahmen notwendig ist, Kontrollmaßnahmen gegenüber Jedermann durchführen zu können. Vor diesem Hintergrund sind auch keine Anforderungen an das Verhalten der zu kontrollierenden Person, die an dem bestimmten Ort angetroffen werden, zu stellen. Besondere Gefahrenlagen, wie z.B. der Drogenhandel in einer offenen Drogenszene und das Ausweichverhalten von Drogendealern, begründen den Bedarf für eine polizeiliche Kontrollmöglichkeit unabhängig von der Dauer des Aufenthalts in dem gefährdeten Bereich. Hierzu hat das Verwaltungsgericht Hamburg im Urteil vom 24. Februar 2000 (4 VG 2471/99) zutreffend ausgeführt, daß Straßendealer gerade nicht an einem Ort verweilen, sondern bestrebt sind, sich möglichst nicht von normalen Passanten zu unterscheiden, die nicht verweilen, sondern einen Bereich zügig durchschreiten. Eine Unterscheidung zwischen Störern und Nichtstörern ist somit gerade nicht möglich.

3

Absatz 2 ermächtigt die Polizei, bei Vorliegen bestimmter Lagebilder Anhalte- und Sichtkontrollen sowie Identitätsfeststellungen im öffentlichen Raum durchzuführen. Die Freie und Hansestadt Hamburg ist eine der Metropolen Europas und als solche immer Ziel von organisierter Bandenkriminalität aus dem In- und Ausland. Für überregional agierende Gruppen ist Hamburg interessant, weil es verkehrstechnisch gut angebunden ist. Dies gilt nicht nur für die Landwege, sondern auch für die Wasserstraßen sowie für die nahe Küste. Hinzu kommt, daß Hamburg Verkehrsknotenpunkt zwischen Nord- und Mitteleuropa ist. Diesen Umstand nutzt insbesondere die Organisierte Kriminalität zum Beispiel bei der Einschleusung von Menschen und beim Drogen- und Waffenhandel. Die Öffnung nach Mittel- und Osteuropa hat diese Entwicklung noch verstärkt. Um diesen Erscheinungsformen der Kriminalität wirksam begegnen zu können, ist es daher erforderlich, bei entsprechenden Lagebildern auch die Verkehrswege in die polizeiliche Kontrolltätigkeit einzubeziehen. Darüber hinaus können besondere Entwicklungen in einzelnen Stadtgebieten entsprechende Kontrollen erforderlich machen wie zum Beispiel Einbruchsserien oder besondere Ausprägungen von Gewaltdelikten. Auch hier soll die Polizei die Möglichkeit haben, in bestimmten, entsprechend dem Lagebild zu definierenden Gebieten Personen anzuhalten und ihre Identität festzustellen. Die Identitätsfeststellung dient in erster Linie dazu, eine von der kontrollierten Person möglicherweise ausgehende Gefahr abzuwehren. Daneben kann die Aufhebung der Anonymität bei potentiellen Störern zum Verzicht auf bestimmte Aktivitäten führen. Die Befugnis zur Inaugenscheinnahme mitgeführter Sachen soll es der Polizei ermöglichen zu klären, ob beispielsweise Einbruchswerkzeug oder Waffen transportiert werden. Die Kontrolle ist zulässig, wenn auf Grund von konkreten Lageerkenntnissen in einem bestimmten Gebiet mit Straftaten von erheblicher Bedeutung zu rechnen ist. Das Lagebild und die hierzu im Einzelnen zu erlassenden Verfahrensregelungen stellen einen Ausgleich zu dem bei anonymen Gefahrenlagen naturgemäß fehlenden individuellen Zurechnungszusammenhang dar und machen die Maßnahme hinreichend bestimmt (vgl. Urteil des Verfassungsgerichtshofs des Freistaates Sachsen vom 10. Juli 2003 - Vf. 43-II-00 - und Entscheidung des Bayerischen Verfassungsgerichtshofs vom 28. März 2003 - Vf. 7-VII-00 -). Der Unterschied zu der Regelung in Absatz 1 Nummer 2 a) besteht einerseits in der Beschränkung auf den öffentlichen Raum, andererseits im Verzicht auf den engen Ortsbezug. Um bei bestimmten Lagebildern adäquat vorbeugend reagieren zu können, kann es erforderlich sein, auch umgrenzte Gebiete zu

kontrollieren, während von Absatz 1 Nummer 2 a) insbesondere auch nicht der Allgemeinheit zugängliche abgeschlossene Räumlichkeiten wie Gaststätten etc. erfasst werden. Die Lageerkenntnisse sind vorab von der Polizei zu dokumentieren, um eine nachträgliche Überprüfung der Maßnahme zu ermöglichen. Die Kontrollen selbst werden in einem gestuften Verfahren durchgeführt. Zunächst erfolgt die Festlegung von Ort und Zeit der Kontrolle. Diese Entscheidung wird bestimmten Funktionsträgern, zum Beispiel dem jeweiligen Leiter eines Polizeikommissariats, übertragen. Daran schließt sich die Auswahl der zu Kontrollierenden an. Von einer solchen Kontrolle wird daher nicht jede beliebige Person erfasst, die sich im öffentlichen Raum bewegt, sondern die Kontrolle orientiert sich an der lageabhängigen Zielgruppe. Die Polizei darf bei der Kontrolle eine Person kurzfristig anhalten, nach ihrer Identität befragen und sich mitgeführte Ausweisdokumente aushändigen lassen. Wird im Falle nicht mitgeführter Ausweisdokumente die Angabe der Personalien verweigert oder bestehen Zweifel an den gemachten Angaben, kann die Person festgehalten, nach mitgeführten Sachen, die der Identitätsfeststellung dienen, durchsucht und zur Dienststelle gebracht werden. Die Auswahl der jeweils erforderlichen Maßnahmen erfolgt unter strikter Wahrung des Verhältnismäßigkeitsgrundsatzes. Die Durchführung von erkennungsdienstlichen Maßnahmen wird ausdrücklich ausgeschlossen. Unabhängig davon darf die Polizei mitgeführte Sachen in Augenschein nehmen. Bei der Inaugenscheinnahme handelt es sich nicht um eine Durchsuchung des Betroffenen. Vielmehr sollen die mitgeführten Sachen lediglich genauer betrachtet werden, ohne tiefer in die Privatsphäre einzudringen. Dies kann beispielsweise im Öffnen einer Tasche oder eines Kofferraums bestehen. Wenn jedoch durch die Inaugenscheinnahme der mitgeführten Sachen eine Gefahr erkannt wird oder ein Verdacht entsteht, kann die Polizei in einem solchen Fall auf Grund der weitergehenden Befugnisse zur Gefahrenabwehr vorgehen.

4

Absatz 4 bezeichnet die zur Identitätsfeststellung zulässigen Mittel. Der Grundsatz der Verhältnismäßigkeit gebietet die in Satz 3 enthaltenen Einschränkungen für die Maßnahmen nach Satz 2 Nummern 4 bis 6. Berechtigungsscheine im Sinne von Absatz 5 sind die für die Ausübung bestimmter Tätigkeiten erforderlichen Nachweise (z.B. Jagd- oder Waffenschein, Reisegewerbekarte, Führerschein). Die einschlägigen Gesetze sehen zwar durchweg vor, daß diese Papiere zuständigen Personen auf Verlangen auszuhändigen sind. Mit dieser Bestimmung wird klargestellt, daß diese Verpflichtung auch gegenüber der Polizei gilt. Erlaubnisbescheide, deren Mitführung durch Auflage vorgeschrieben wird, sind z.B. Sondernutzungen nach dem Wegegesetz.

§ 5 Datenerhebung zur Vorbereitung auf die Hilfeleistung in Gefahrenfällen
(1) Die Polizei darf über
1. **Personen, deren besondere Kenntnisse oder Fähigkeiten zur Gefahrenabwehr benötigt werden,**
2. **Verantwortliche für Anlagen oder Einrichtungen, von denen eine erhebliche Gefahr ausgehen kann,**
3. **Verantwortliche für gefährdete Anlagen oder Einrichtungen,**
4. **Verantwortliche für Veranstaltungen in der Öffentlichkeit**

Namen, Vornamen, akademische Grade, Anschriften, Telefonnummern und andere Informationen über die Erreichbarkeit sowie nähere Angaben über die

Zugehörigkeit zu einer der genannten Personengruppen erheben, soweit dies zur Vorbereitung auf die Hilfeleistung in Gefahrenfällen erforderlich ist. Eine verdeckte Datenerhebung ist unzulässig.
(2) Die nach Absatz 1 Satz 1 Nummer 4 erhobenen personenbezogenen Daten, die in Dateien suchfähig gespeichert wurden, und Akten, die zur Person des Verantwortlichen angelegt wurden, sind spätestens einen Monat nach Beendigung des Anlasses zu löschen oder zu vernichten, sofern es sich nicht um regelmäßig wiederkehrende Veranstaltungen handelt.

Die Polizei kann vielfach - soweit sie im Rahmen ihrer Eilzuständigkeit tätig wird - in Gefahrenfällen nur wirkungsvoll Hilfe leisten, wenn sie Personen, die über die für die Bewältigung einer Gefahrenlage erforderlichen Fähigkeiten oder Fertigkeiten verfügen, schnellstmöglich erreichen kann. Hierzu gehören z.B. Hausmeister oder Sicherheitstechniker einer großtechnischen Anlage, aber z.B. auch Abschleppunternehmer, Sachverständige oder Dolmetscher. Der betroffene Personenkreis und die zu erhebenden Daten sind auf das unbedingt erforderliche Maß zu begrenzen. Darüber hinaus wird nach Absatz 1 Satz 2 eine verdeckte Datenerhebung ausgeschlossen. Die Speicherung von Daten der in Absatz 1 Satz 1 Nummer 4 genannten Personen (z.B. Veranstalter einer großen Sportveranstaltung) ist grundsätzlich nur befristet möglich. Ausnahmen sind bei regelmäßig wiederkehrenden Veranstaltungen zugelassen (z.B. Teilnahme eines Sportvereins am Punktspielbetrieb). Suchfähig gespeicherte Daten im Sinne von Absatz 2 sind solche, die unter Verwendung des Namens, eines personenbeziehbaren Aktenzeichens oder eines Hilfsmerkmals jederzeit gezielt aufgefunden werden können.

§ 6 Voraussetzungen der Datenerhebung
Die Polizei darf personenbezogene Daten erheben,

1. **soweit es im Einzelfall erforderlich ist zur Abwehr einer bevorstehenden Gefahr, zur Wahrnehmung grenzpolizeilicher Aufgaben oder einer Aufgabe der Amts- oder Vollzugshilfe,**
2. **wenn die Daten aus allgemein zugänglichen Quellen entnommen werden können und dies zur Erfüllung ihrer Aufgaben erforderlich ist,**
3. **wenn dies zur Vorbereitung und Durchführung eines Einsatzes erforderlich ist, bei dem erfahrungsgemäß eine besondere Gefährdungslage besteht,**
4. **wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass die Person Opfer einer Straftat werden wird, und dies zur Wahrnehmung der Schutzaufgabe erforderlich ist,**
5. **wenn die Person sich im räumlichen Umfeld einer Person aufhält, die auf Grund ihrer beruflichen Tätigkeit oder ihrer Stellung in der Öffentlichkeit besonders gefährdet erscheint, und dies zum Schutz der gefährdeten Person erforderlich ist,**
6. **wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass die Person künftig Straftaten begehen wird, und die Erhebung zur vorbeugenden Bekämpfung von Straftaten mit erheblicher Bedeutung erforderlich ist,**
7. **über Kontakt- oder Begleitpersonen, wenn dies zur vorbeugenden Bekämpfung von Straftaten mit erheblicher Bedeutung erforderlich ist.**

1

Die Vorschrift regelt die tatbestandlichen Voraussetzungen der Datenerhebung. In welcher Form die Datenerhebung erfolgt, ergibt sich aus § 2. Ob eine andere öffentliche Stelle der Polizei Daten übermitteln darf oder muß, ergibt sich aus den für sie maßgeblichen Rechtsvorschriften. Eine Regelung in dieser Form ist erforderlich, weil die polizeiliche Generalklausel weder als Rechtsgrundlage für die Datenerhebung konzipiert ist, noch den heutigen verfassungsrechtlichen Anforderungen an eine bereichsspezifische Rechtsgrundlage entspricht. Insbesondere würde diese Vorschrift nur Datenerhebungen bei einer konkreten Gefahr zulassen, die sich grundsätzlich auch nur auf Verantwortliche (vgl. § 3) beziehen dürften. Die Polizei muß jedoch, wenn sie ihre Aufgaben wirkungsvoll erfüllen soll, auch die Daten anderer Personen (z.B. einer Person, bei der sich der Fahrzeugführer eines verkehrsbehindernd abgestellten Fahrzeuges aufhält) erheben können und in bestimmten eng abgegrenzten Situationen auch schon im Vorfeld konkreter Gefahren tätig werden dürfen (§ 6 Nummern 4 bis 7). Nummer 1 setzt ebenso wie § 4 Absatz 1 Nummer 1 eine bevorstehende Gefahr voraus. Datenerhebungen „ins Blaue hinein“ sind damit grundsätzlich ausgeschlossen. Entsprechend dem Sprachgebrauch in den Polizeigesetzen anderer Länder gehört zur Abwehr einer bevorstehenden Gefahr sowohl die Feststellung von Gefahren, wenn Anhaltspunkte für die Entwicklung einer Gefahrenlage gegeben sind, als auch die Beseitigung einer bereits eingetretenen Störung, wenn von ihr weiterhin eine Gefahr ausgeht. Die Datenerhebung nach Nummer 1 soll außerdem die sachgerechte Vorbereitung einer Maßnahme der Amts- oder Vollzugshilfe ermöglichen. Der Tatbestand in Nummer 2 dient vorrangig der Klarstellung. Denn zum einen kann davon ausgegangen werden, daß der Betroffene seine Daten selbst preisgegeben hat und somit damit einverstanden ist, daß andere Personen oder Stellen - also auch die Polizei - hiervon Kenntnis nehmen. Zum anderen wird die Auswertung allgemein zugänglicher Quellen nicht ohne einen bestimmten Anlaß erfolgen, so daß sich die Polizei in der Regel auf einen anderen Befugnistatbestand für die Erhebung dieser Daten stützen kann. Anlässe im Sinne der Nummer 3 liegen insbesondere vor, wenn bei vergleichbaren Anlässen in der Vergangenheit eine Gefährdung der öffentlichen Sicherheit eingetreten ist, die Anlaß zu polizeilichem Einschreiten gab. So muß die Polizei z.B. anläßlich eines bevorstehenden Fußballspiels, bei dem mit gewalttätigen Auseinandersetzungen zwischen "Fan-Clubs" zu rechnen ist, Angaben über die Anzahl der zu erwartenden Anhänger der Gastmannschaft und deren bisheriges Verhalten bei früheren Spielen erheben können, um auf Gewalttätigkeiten rechtzeitig reagieren zu können.

2

Die Erhebungstatbestände in den Nummern 4 und 5 sollen der Polizei die Möglichkeit geben, Schutzaufgaben gegenüber gefährdeten Personen wahrnehmen zu können. Nummer 4 betrifft insbesondere Fälle, in denen eine Person mit einer Straftat bedroht wird oder die Polizei Hinweise erhält, daß eine Straftat gegen diese Person geplant wird. Hier kann z.B. eine Beobachtung oder Befragung von Angehörigen, Nachbarn oder Kollegen erforderlich sein. Nummer 5 erlaubt die Datenerhebung über Personen, die sich im räumlichen Umfeld einer anderen Person aufhalten, die als besonders gefährdet einzustufen ist (z.B. Politiker, Angehörige des öffentlichen Dienstes in besonders herausgehobener Stellung oder Führungskräfte der Wirtschaft). Nach dieser Bestimmung wäre es z.B. zulässig, das Personal eines Hotels zu überprüfen, in dem ein ausländischer Staatsgast untergebracht ist.

Nummer 6 betrifft die Fälle, in denen zwar tatsächliche Anhaltspunkte die Annahme einer von einer bestimmten Person geplanten Straftat rechtfertigen, diese Hinweise sich aber weder zu einer bevorstehenden Gefahr im Sinne der Nummer 1 noch zu dem Anfangsverdacht einer Straftat verdichtet haben. Dieser Tatbestand ist erforderlich, da die Polizei sonst so lange von einem Einschreiten bzw. einer Klärung des Sachverhalts absehen müßte, bis sich die tatsächlichen Anhaltspunkte zu einer bevorstehenden Gefahr im Sinne der Nummer 1 oder des Anfangsverdachts einer - zumindest versuchten - Straftat verdichtet hätten. Dann wäre es jedoch möglicherweise für ein wirkungsvolles Einschreiten der Polizei zu spät. Tatsächliche Anhaltspunkte im Sinne dieser Bestimmung können sich insbesondere aus laufenden polizeilichen Ermittlungsverfahren oder aus Hinweisen Dritter ergeben. Nummer 7 erlaubt darüber hinaus auch die Erhebung der Daten von Kontakt- oder Begleitpersonen der in Nummer 6 genannten Personen. Aus der Begriffsbestimmung in § 1 Absatz 6 ergibt sich zugleich, daß diese Vorschrift nicht die gezielte Datenerhebung über jede beliebige Person erlaubt, die Kontakt zu einem potentiellen Straftäter hat.

Zweiter Abschnitt

Besondere Befugnisse zur Datenerhebung

§ 7 Erkennungsdienstliche Maßnahmen

(1) Die Polizei darf erkennungsdienstliche Maßnahmen durchführen

1. **zum Zweck der Identitätsfeststellung (§ 4 Absatz 4), wenn dies auf andere Weise nicht oder nur unter erheblichen Schwierigkeiten möglich ist,**
2. **zur vorbeugenden Bekämpfung von Straftaten, wenn der Betroffene verdächtig ist, eine mit Strafe bedrohte Tat begangen zu haben, und wegen der Art oder Ausführung der Tat sowie der Persönlichkeit des Betroffenen die Gefahr der Begehung weiterer Straftaten besteht.**

(2) Ist die Identität festgestellt, sind in den Fällen des Absatzes 1 Nummer 1 die im Zusammenhang mit der Feststellung angefallenen Unterlagen zu vernichten, es sei denn, ihre weitere Aufbewahrung ist für Zwecke nach Absatz 1 Nummer 2 oder nach anderen Rechtsvorschriften zulässig.

(3) Erkennungsdienstliche Maßnahmen sind

1. **die Abnahme von Finger- und Handflächenabdrücken,**
2. **die Aufnahme von Lichtbildern,**
3. **die Feststellung äußerlich wahrnehmbarer Merkmale,**
4. **Messungen.**

Soweit es zur Feststellung der Identität erforderlich ist, darf die Polizei auch Befragungen anderer Personen vornehmen und Urkunden oder sonstige Unterlagen einsehen. Regelungen über ein Berufs- oder besonderes Amtsgeheimnis bleiben unberührt. Erkennungsdienstliche Maßnahmen dürfen nur von besonders ermächtigten Bediensteten angeordnet werden.

(4) Der Betroffene darf zur Durchführung erkennungsdienstlicher Maßnahmen vorgeladen und, wenn er der Vorladung ohne hinreichenden Grund nicht folgt, zwangsweise vorgeführt werden.

(5) Ist eine Identitätsfeststellung unbekannter Toter auf andere Weise nicht möglich, darf die Polizei DNA-Material von vermissten Personen und unbekannten Toten sicherstellen und molekulargenetische Untersuchungen

durchführen. Das erlangte DNA-Identifizierungsmuster kann zu diesem Zweck in einer Datei gespeichert werden. Eine Nutzung für andere Zwecke ist nicht zulässig. Molekulargenetische Untersuchungen bedürfen der richterlichen Anordnung. Zuständig ist das Amtsgericht Hamburg. Das Verfahren richtet sich nach den Vorschriften des Gesetzes über die Freiwillige Gerichtsbarkeit. § 81f Absatz 1 Satz 3 und Absatz 2 der Strafprozessordnung gilt entsprechend.

1

Regelungen über die Zulässigkeit erkennungsdienstlicher Maßnahmen sind bereits in der Strafprozeßordnung enthalten. Nach § 81b StPO sind diese bei Beschuldigten zulässig, soweit die Maßnahrnen für Zwecke der Durchführung des Strafverfahrens oder für die Zwecke des Erkennungsdienstes notwendig sind. Absatz 1 Nummer 1 läßt erkennungsdienstliche Maßnahmen als "ultima ratio" der Identitätsfeststellung zu, wenn andere Möglichkeiten nicht oder nicht mit zumutbarem Aufwand bestehen. Absatz 1 Nummer 2 enthält in Ergänzung zu Nummer 1 die ebenfalls der Gefahrenabwehr dienende Ermächtigungsgrundlage für erkennungsdienstliche Maßnahmen zur vorbeugenden Bekämpfung von Straftaten. Hierzu gehören auch die Fälle, in denen bereits eine Bestrafung erfolgte oder eine Verurteilung mangels Schuldfähigkeit nicht erfolgen konnte. Von Bedeutung ist dies für die erkennnungsdienstliche Behandlung Strafunmündiger sowie für rechtskräftig Verurteilte, weil beide Personengruppen schon begrifflich nicht bzw. nicht mehr Beschuldigte sind und somit auch nicht in den Anwendungsbereich des § 81b StPO fallen. Die Zulässigkeit erkennungsdienstlicher Maßnahmen wird in dieser Vorschrift ausdrücklich auf Fälle der Wiederholungsgefahr beschränkt. Hierdurch soll der gefahrenabwehrende Charakter verdeutlicht werden.

2

Die Regelung in Absatz 2 entspricht § 163c Absatz 4 StPO. Im übrigen bestimmt sich die weitere Aufbewahrung und Nutzung nach den Bestimmungen des Dritten Abschnitts (§§ 14 bis 27). Die im Musterentwurf enthaltene Regelung, wonach der Betroffene bei Wegfall der Voraussetzungen die Vernichtung der Unterlagen verlangen kann, ist nicht übernommen worden, da hierdurch der mißverständliche Eindruck entstehen könnte, die Vernichtung habe nur auf Antrag des Betroffenen zu erfolgen. Vielmehr hat die Polizei nach den Bestimmungen des Dritten Abschnitts von sich aus - also von Amt wegen - die Erforderlichkeit der weiteren Speicherung zu prüfen.

3

Absatz 3 enthält eine notwendige Begriffsbestimmung. Die Aufzählung ist allerdings nicht abschließend. Auch andere Methoden sind nach Absatz 3 Nummer 3 zulässig, soweit sie sich auf die Feststellung äußerlich wahrnehmbarer Merkmale beschränken, also nicht mit Eingriffen in die körperliche Unversehrtheit verbunden sind. Der Verweis auf Berufs- oder besondere Amtsgeheimnisse verdeutlicht, daß eine Einsichtnahme in Urkunden oder sonstige Unterlagen, die einem solchen Geheimnis unterliegen, nur zulässig ist, soweit der jeweilige Zweck nicht entgegensteht. Absatz 4 erlaubt es der Polizei unter den dort genannten Voraussetzungen, eine Person zur Durchführung erkennungsdienstlicher

Maßnahmen vorzuladen und gegebenenfalls vorzuführen. Hinsichtlich des Richtervorbehalts wird auf die Kommentierung zu § 13a HmbSOG verwiesen.

4

Absatz 5 regelt die Nutzung der DNA-Analyse zu Zwecken der Vermißten-sachbearbeitung und der Identifizierung unbekannter Toter. Es kommt in der polizeilichen Praxis immer wieder vor, daß nicht identifizierbare Leichen aufgefunden werden, bei denen angesichts eines fortgeschrittenen Verwesungszustandes eine andere Möglichkeit der Identifizierung (z.B. über Fotos, Fingerabdrücke, Gebissabdruck) unmöglich ist. Die DNA bleibt aber theoretisch unbegrenzt haltbar und bietet zudem die einzige Möglichkeit, auch Leichenteile sicher zuzuordnen. Gleiches gilt auch für die Identifizierung von Opfern in Katastrophenfällen, wie z.B. Flugzeugabstürzen, schweren Bahnunglücken oder Brandkatastrophen. Um die Identität unbekannter Toter und das Schicksal Vermisster außerhalb strafrechtlicher Ermittlungsverfahren klären zu können, ist ein Abgleich des DNA-Materials erforderlich. Zwar ist die DNA-Analyse, die der Vorsorge für die künftige Strafverfolgung dient, in wesentlichen Teilen bundesgesetzlich geregelt (siehe § 81g StPO). Es handelt sich allerdings nicht um eine abschließende Regelung, sondern es verbleibt, soweit nicht eine bundesgesetzliche Regelung einschlägig ist, für den Personenkreis der Nicht-Beschuldigten eine landesrechtliche Regelungskompetenz. Die Speicherung der erlangten DNA-Identifizierungsmuster ist zweckmäßig und auch erforderlich, da ansonsten ein Datenabgleich mit anderen Proben nicht möglich wäre. Die molekulargenetische Untersuchung bedarf der richterlichen Anordnung. Sie muß schriftlich erfolgen und den mit der Untersuchung beauftragten Sachverständigen benennen.

§ 8 Datenerhebung im öffentlichen Raum und an besonders gefährdeten Objekten

(1) Die Polizei darf bei oder im Zusammenhang mit öffentlichen Veranstaltungen oder Ansammlungen personenbezogene Daten, auch durch den Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufzeichnungen über die für eine Gefahr Verantwortlichen erheben, wenn Tatsachen die Annahme rechtfertigen, dass dabei Straftaten begangen werden. Die Maßnahme darf auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden. Bild- und Tonaufzeichnungen, in Dateien suchfähig gespeicherte personenbezogene Daten sowie zu einer Person suchfähig angelegte Akten sind spätestens einen Monat nach der Datenerhebung zu löschen oder zu vernichten. Dies gilt nicht, wenn die Daten zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung oder Straftaten benötigt werden oder Tatsachen die Annahme rechtfertigen, dass die Person künftig Straftaten begehen wird, und die Aufbewahrung zur vorbeugenden Bekämpfung von Straftaten mit erheblicher Bedeutung erforderlich ist.

(2) Die Polizei darf an oder in den in § 4 Absatz 1 Nummer 3 genannten Objekten Bild- und Tonaufzeichnungen über die für eine Gefahr Verantwortlichen anfertigen, soweit Tatsachen die Annahme rechtfertigen, dass an oder in Objekten dieser Art Straftaten begangen werden sollen, durch die Personen, diese Objekte oder andere darin befindliche Sachen gefährdet sind. Absatz 1 Sätze 2 bis 4 gilt entsprechend. Auf den Einsatz von

Aufzeichnungsgeräten ist hinzuweisen, soweit dadurch nicht der Zweck der Maßnahme gefährdet wird.
(3) Die Polizei darf öffentlich zugängliche Orte mittels Bildübertragung und -aufzeichnung offen beobachten, soweit an diesen Orten wiederholt Straftaten begangen worden sind und Tatsachen die Annahme rechtfertigen, dass dort auch künftig mit der Begehung von Straftaten zu rechnen ist. Absatz 1 Sätze 2 bis 4 gilt entsprechend.
(4) Die Polizei darf von Personen, die sich in amtlichem Gewahrsam befinden, durch den offenen Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufzeichnungen Daten erheben, wenn dies zum Schutz der Betroffenen oder der Vollzugsbediensteten oder zur Verhütung von Straftaten in polizeilich genutzten Räumen erforderlich ist. Die Maßnahme darf auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden. Besuche von Verteidigern werden nicht überwacht. Bild- und Tonaufzeichnungen sind unverzüglich zu löschen, soweit sie nicht für Zwecke der Strafverfolgung benötigt werden.
(5) Die Polizei darf bei Anhalte- und Kontrollsituationen im öffentlichen Verkehrsraum durch den offenen Einsatz technischer Mittel zur Anfertigung von Bild und Tonaufzeichnungen Daten erheben, wenn dies zum Schutz der Vollzugsbediensteten oder eines Dritten erforderlich ist. Absatz 4 Sätze 2 und 4 gilt entsprechend.
(6) Die Polizei darf bei Kontrollen im öffentlichen Verkehrsraum nach diesem Gesetz und anderen Gesetzen personenbezogene Daten durch den offenen Einsatz technischer Mittel zur elektronischen Erkennung von Kraftfahrzeugkennzeichen zum Zwecke des automatisierten Abgleichs mit dem Fahndungsbestand erheben. Eine verdeckte Datenerhebung ist nur zulässig, wenn durch die offene Datenerhebung der Zweck der Maßnahme gefährdet würde. Daten, die im Fahndungsbestand nicht enthalten sind, sind unverzüglich zu löschen.
(7) § 17 und § 24 Absatz 4 bleiben unberührt.

1

Absatz 1 enthält eine Standardermächtigung für Maßnahmen im Vorfeld einer Gefahrensituation. Ein Teil der Vorfeldaktivitäten der Polizei in diesem Bereich enthält zwar noch keinen Grundrechtseingriff (z.B. die Anfertigung von Übersichtsaufnahmen). Wegen der gerade bei Bildaufzeichnungen sehr schwierigen Abgrenzung gegenüber einer gezielten Datenerhebung werden allerdings auch diese Maßnahmen von dieser Befugnisnorm mit abgedeckt. Derartige Maßnahmen sind notwendig, da hierdurch Straftaten bei öffentlichen Veranstaltungen oder Ansammlungen wirksam verhindert werden können. Beispielsweise nutzen Fußballrowdies bei Spielen der Bundesliga den Schutz der Menge, um Schlägereien mit Anhängern der gegnerischen Mannschaft zu beginnen oder um Wurfgeschosse (z.B. Flaschen, Feuerwerkskörper) auf das Spielfeld oder auf die Anhänger der gegnerischen Mannschaft zu werfen. Solche Ausschreitungen sind vielfach das Ergebnis einer Eskalation. Zur Gewährleistung einer effektiven Gefahrenabwehr ist es daher unabweisbar, z.B. die Brennpunkte oder den jeweiligen Aufenthaltsort als gewalttätig bekannter Besucher zu beobachten. Aus der Formulierung „bei oder im Zusammenhang mit“ ergibt sich, daß für die Datenerhebung ein enger zeitlicher oder räumlicher Zusammenhang zum jeweiligen Anlaß (öffentliche Veranstaltung oder Ansammlung) erforderlich ist. Insbesondere zählt hierzu die Anreise oder Abreise zu dem Anlaß. Zulässig wäre danach z.B. auch die Beobachtung als gewalttätig

bekannter Fan-Gruppen am Treffpunkt vor ihrer Abreise zu einem Auswärtsspiel ihrer Mannschaft. Die übrigen Befugnisse zur Datenerhebung (z.B. nach den §§ 4 bis 6) oder nach der Strafprozeßordnung bleiben hierdurch unberührt. Absatz 1 Sätze 3 und 4 enthalten eine Vernichtungs- bzw. Löschungsregelung. Diese ist beschränkt auf suchfähige Daten, da eine Vernichtung aller bei dem jeweiligen Anlaß erstellten Unterlagen (z.B. Einsatzbefehle oder Erfahrungsberichte) zu einer erheblichen Beeinträchtigung polizeilicher Belange führen würde. Eine weitere Aufbewahrung nach Absatz 1 Satz 4 z.B. von Lichtbildern kann insbesondere erforderlich sein, um diese Personen künftig bei ähnlichen Anlässen erkennen zu können und wirksame Gegenmaßnahmen zu ergreifen.

2

Die in Absatz 2 geregelte Anfertigung von Bild- und Tonaufzeichnungen an oder in besonders gefährdeten Objekten erfolgt in der Regel durch die jeweils Verantwortlichen (z.B. Inhaber eines Parkhauses, in dem häufig Fahrzeuge gestohlen oder aufgebrochen werden). Die Polizei hat nach geltendem Recht die Befugnis, zur Aufklärung bestimmter Straftaten auf die hierbei angefallenen Unterlagen Zugriff zu nehmen. Um einer rechtspolitisch bedenklichen Privatisierung der Verbrechensbekämpfung vorzubeugen, soll mit dieser Bestimmung auch der Polizei das Recht eingeräumt werden, aus eigener Initiative unter den hier genannten Voraussetzungen Aufzeichnungsgeräte einzusetzen. Auf den Einsatz von Aufzeichnungsgeräten ist grundsätzlich in geeigneter Weise hinzuweisen. Eine Ausnahme ist zulässig, wenn durch den Hinweis der Zweck der Maßnahme gefährdet wird, z.B. potentiellen Straftätern Gelegenheit gegeben wird, die Maßnahme durch entsprechendes Verhalten zu unterlaufen.

3

Absatz 3 enthält die Rechtsgrundlage für Bildübertragungen und -aufzeichnungen an öffentlich zugänglichen Straßen und Plätzen, soweit an diesen Orten wiederholt Straftaten begangen worden sind und Tatsachen die Annahme rechtfertigen, daß auch künftig mit der Begehung von Straftaten zu rechnen ist. Die Videoüberwachung hat offen zu erfolgen. Die Videoüberwachung an öffentlich zugänglichen Orten soll sowohl in Form der bloßen Bildübertragung als auch der Bildaufzeichnung vorgenommen werden dürfen. Während bei der Bildübertragung die Bilder lediglich durchlaufen und von einem Polizeibeamten beobachtet werden, werden mit der Bildaufzeichnung Daten der Betroffenen erhoben. Es handelt sich um Eingriffe in die informationelle Selbstbestimmung, von denen sehr viele Personen betroffen sein können, wenn der videoüberwachte Ort von zentraler Bedeutung ist und ein großes Aufkommen an Passanten und Besuchern hat. In den weitaus meisten Fällen handelt es sich um Personen, von denen keine Gefahr ausgeht und denen selbst auch keine Gefahr droht. Die Eingriffe sind daher nur unter strengen Anforderungen zulässig. So dürfen nur öffentlich zugängliche Straßen und Plätze überwacht werden. Darüber hinaus müssen in der Vergangenheit an diesem Ort wiederholt Straftaten begangen worden sein. Das bedeutet, daß an dem zu überwachenden Ort mehrere Straftaten verübt worden sein müssen und diese auch noch in einem angemessenen zeitlichen Zusammenhang zueinander stehen müssen. Dabei gilt der Grundsatz, daß die Anforderungen an Häufigkeit und zeitliche Nähe in dem Maße sinken, in dem der drohende Schaden steigt. Es handelt sich um eine Entscheidung im Einzelfall, die immer unter Berücksichtigung des Verhältnismäßigkeitsprinzips getroffen werden muß. Zusätzlich bedarf es einer Gefahrenprognose. Es müssen

demnach Tatsachen die Annahme rechtfertigen, daß auch zukünftig Straftaten an diesem Ort begangen werden. Damit sind bloße Vermutungen nicht ausreichend. Vielmehr muss auf Grund polizeilicher Lageerkenntnisse oder anderer nachprüfbarer Tatsachen damit zu rechnen sein, daß an dem Ort noch weitere Straftaten begangen werden. Auch hier muss ein angemessener zeitlicher Zusammenhang bestehen. Diese Bestimmung der zu überwachenden Örtlichkeiten korrespondiert mit dem Ziel der Maßnahme, nämlich der Verhütung von Straßenkriminalität und der Stärkung des Sicherheitsgefühls der Bevölkerung. Eine Beschränkung der Örtlichkeiten etwa auf gefährliche Orte im Sinne des § 4 Absatz 1 Nummer 2 oder Absatz 2 würde die Möglichkeiten der Videoüberwachung in nicht gebotener Weise einschränken, da eine Reihe von Deliktsbereichen in diesem Fall unberücksichtigt bleiben müsste. Bei Sachbeschädigungen, Diebstählen, Autoaufbrüchen u.ä. handelt es sich in der Regel nicht um Straftaten von erheblicher Bedeutung und doch tangieren diese Delikte das Sicherheitsgefühl der Bevölkerung in erheblichem Maße. Mit der Ergänzung in Absatz 1 Satz 4 wird gewährleistet, daß die Bildaufzeichnungen auch zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung gespeichert werden dürfen. Die Aufzeichnungen sollen also nicht für die Verfolgung geringfügiger Ordnungswidrigkeiten, sondern nur für jene Ordnungswidrigkeiten Verwendung finden, die sich gegen ein besonders bedeutsames Interesse der Allgemeinheit richten und die von der Öffentlichkeit in besonderer Weise als störend empfunden werden. Damit soll zum Beispiel die Verfolgung von aufgezeichneten Graffiti-Schmierereien, die gegenwärtig nicht als Straftaten zu bewerten sind, oder auch von größeren Müllablagerungen ermöglicht werden. Die in Absatz 1 Satz 3 geregelte Monatsfrist, nach der die erhobenen Daten spätestens zu löschen sind, wenn sie nicht für ausdrücklich benannte Zwecke benötigt werden, gilt auch für die Videoüberwachung nach Absatz 3. Erfahrungen haben gezeigt, daß Straftaten zum Teil erst verzögert zur Anzeige gelangen. Eine zu schnelle Löschung würde in diesen Fällen die Verfolgung der Tat unnötig erschweren.

4

Die Regelung des Absatzes 4 ist erforderlich, um Sachbeschädigungen und Verletzungen in polizeilich genutzten Räumen (z.B. Zellen, Durchsuchungsräumen, sog. Sicheren Räumen, Gefangenentransportzellen, angemietete Sammelzellen bei besonderen Anlässen) möglichst zu verhindern. Gegenwärtig werden nahezu täglich Sachbeschädigungen durch verwahrte Personen verübt. Der Ersatz des entstandenen Schadens kann in vielen Fällen von den Verursachern nicht erlangt werden, da diesen häufig die finanziellen Mittel fehlen. Außerdem kommt es regelmäßig zu Widerstandshandlungen durch verwahrte Personen, durch die die eingesetzten Bediensteten gefährdet bzw. verletzt werden. Des Weiteren kommt es sowohl in den Verwahrräumen der Polizeigebäude als auch in den Zellen der Gefangenentransportfahrzeuge immer wieder zu Eigenverletzungen und Suizidversuchen durch verwahrte Personen. Um dieses rechtzeitig verhindern zu können, ist eine dauerhafte Überwachung der jeweiligen Örtlichkeiten zum Schutz der Personen erforderlich, die personell und auf Grund der räumlichen Gegebenheiten unmöglich ist. Es ist davon auszugehen, daß die offene Videoüberwachung verwahrter Personen potentielle Täter abschreckt, eventuelle Taten durch früheres Erkennen verhindert werden oder im Fall einer Tat die Beweislage vor Gericht erheblich verbessert wird und sich dadurch sowohl die Anzahl verletzter Personen (Bediensteter und Verwahrter) als auch die Anzahl der Sachbeschädigungen an Amtsgebäuden und deren Einrichtung reduzieren läßt.

5

Die Regelung in Absatz 5 trägt den Empfehlungen der Projektgruppen „Eigensicherung in der polizeilichen Praxis“ und „Gewalt gegen Polizeivollzugsbeamtinnen und -beamte“ des Arbeitskreises II der Ständigen Konferenz der Innenminister und -senatoren aus dem Jahr 2000 Rechnung. Vor dem Hintergrund der gestiegenen Gewaltbereitschaft gegenüber Polizeibeamten sind Videoaufzeichnungen zur Dokumentation von Anhalte- und Kontrollsituationen im öffentlichen Verkehrsraum für sinnvoll erachtet worden. Die Befugnis soll in erster Linie bei Anhaltevorgängen mit Streifenwagen zur Anwendung gelangen und allein der Eigensicherung dienen. In mit Videokameras ausgestatteten Streifenwagen kann in der konkreten Anhaltesituation der Betrieb der Kamera für den Betroffenen erkennbar gestartet werden. Damit soll in erster Linie die Aggressionsbereitschaft gesenkt und das Bewußtsein für Eigensicherungsmaßnahmen bei den Polizeibeamten gestärkt werden.

6

In Absatz 6 wurde eine ausdrückliche Rechtsgrundlage für den präventiv-polizeilichen Einsatz automatischer Kennzeichenlesesysteme im Rahmen von Verkehrskontrollen geschaffen. Danach darf die Polizei bei Kontrollen im öffentlichen Verkehrsraum personenbezogene Daten durch den offenen Einsatz technischer Mittel zur elektronischen Erkennung von Kraftfahrzeugkennzeichen zum Zwecke des automatisierten Abgleichs mit dem Fahndungsbestand erheben. Technisch wird sichergestellt, daß nur die Trefferfälle angezeigt werden. Bei ihnen handelt es sich um gestohlene Kraftfahrzeuge, gestohlene Kraftfahrzeugkennzeichen oder aber um Kraftfahrzeugkennzeichen, die aus sonstigen Gründen ausgeschrieben sind. Dabei ist zu berücksichtigen, daß nicht nur der Diebstahl des betreffenden Kennzeichens oder Fahrzeugs an sich eine Straftat ist, sondern daß diese Kraftfahrzeuge oder Kennzeichen auch zur Begehung weiterer Straftaten verwendet werden. Mit dem Einsatz dieser neuen technischen Möglichkeit können künftig Polizeikontrollen wesentlich effizienter durchgeführt werden. Von besonderer Bedeutung ist darüber hinaus der Aspekt, daß Kennzeichenlesegeräte zur Eigensicherung von Polizeibeamten bei Kontrollen eingesetzt werden können, indem etwa ein vor einer Fahrzeugkontrolle eingesetztes Kennzeichenlesegerät ein Alarmsignal bei den kontrollierenden Beamten auslöst, wenn sich ein zur Fahndung ausgeschriebenes Fahrzeug nähert. Nicht ausgeschriebene Kraftfahrzeugkennzeichen sind dem Zweck der Datenerhebung entsprechend nach dem automatisierten Abgleich unverzüglich zu löschen. Die Eingriffsintensität bei nicht betroffenen Personen ist daher denkbar gering. Ausgeschriebene Kennzeichen können mit den erforderlichen Daten nach den allgemeinen Vorschriften gespeichert und weiterverarbeitet werden.

7

Die Verweisung in Absatz 7 soll klarstellen, daß eine Löschung und Vernichtung der angefertigten Unterlagen unter den dort geregelten Voraussetzungen unterbleiben kann. Hierdurch soll der Polizei insbesondere die Nutzung von Bildaufzeichnungen zur polizeilichen Aus- und Fortbildung erlaubt werden.

§ 9 Datenerhebung durch Observation

(1) Die Polizei darf personenbezogene Daten erheben durch eine planmäßig angelegte Beobachtung, die innerhalb einer Woche länger als 24 Stunden oder über den Zeitraum einer Woche hinaus vorgesehen ist oder tatsächlich durchgeführt wird, (längerfristige Observation)

1. **über die für eine Gefahr Verantwortlichen und unter den Voraussetzungen von § 10 SOG über die dort genannten Personen, wenn dies zur Abwehr einer unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist,**
2. **über Personen, soweit Tatsachen die Annahme rechtfertigen, dass diese Personen Straftaten von erheblicher Bedeutung begehen werden, wenn die Datenerhebung zur vorbeugenden Bekämpfung dieser Straftaten erforderlich ist, sowie über deren Kontakt- oder Begleitpersonen, wenn die Aufklärung des Sachverhaltes auf andere Weise aussichtslos wäre.**

Die Maßnahme darf auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.

(2) Der Einsatz nach Absatz 1 darf nur vom Polizeipräsidenten angeordnet werden. Die Anordnung ist aktenkundig zu machen. Aus der Anordnung müssen sich

1. **Art, Beginn und Ende der Maßnahme; eine Verlängerung ist zulässig, soweit die Voraussetzungen für die Anordnung der Maßnahme fortbestehen,**
2. **an der Durchführung beteiligte Personen,**
3. **Tatsachen, die den Einsatz der Maßnahme begründen,**
4. **Zeitpunkt der Anordnung und Name sowie Dienststellung des Anordnenden**

ergeben.

(3) Personen, gegen die sich Datenerhebungen richteten, sind nach Abschluss der Maßnahme hierüber durch die Polizei zu unterrichten, sobald dies ohne Gefährdung des Zwecks der Datenerhebung geschehen kann. Ist wegen desselben Sachverhalts ein strafrechtliches Ermittlungsverfahren eingeleitet worden, ist die Unterrichtung in Abstimmung mit der Staatsanwaltschaft nachzuholen, sobald dies der Stand des Ermittlungsverfahrens zulässt.

(4) Auf eine Observation, die nicht die in Absatz 1 genannten Voraussetzungen erfüllt (kurzfristige Observation), finden die Absätze 1 bis 3 keine Anwendung. Durch eine kurzfristige Observation darf die Polizei Daten nur erheben, soweit dies zum Zwecke der Gefahrenabwehr (§ 1 Absatz 1) erforderlich ist und ohne diese Maßnahme die Erfüllung der polizeilichen Aufgabe gefährdet wird.

(5) Die Polizei darf unter den Voraussetzungen des Absatzes 1 auch besondere für Observationszwecke bestimmte technische Mittel zur Ermittlung des Aufenthaltsortes des Betroffenen verwenden.

1

Die in dieser Bestimmung geregelte längerfristige Observation gehört zu den besonderen Mitteln der Datenerhebung. Im Interesse der Regelungsklarheit sind die übrigen besonderen Mittel der Datenerhebung (Einsatz technischer Mittel, Einsatz von Vertrauenspersonen und Verdeckten Ermittlern, polizeiliche Beobachtung) jeweils in gesonderten Bestimmungen geregelt. Soweit für die übrigen besonderen Mittel der Datenerhebung gleiche Regelungen gelten sollen, beschränken sich die übrigen Bestimmungen auf eine Verweisung. Absatz 1 enthält zunächst eine Definition der längerfristigen Observation. Sie liegt entweder vor, wenn die planmäßig angelegte Beobachtung innerhalb einer Woche länger als 24 Stunden

(reine Beobachtungszeit) andauert oder über den Zeitraum einer Woche hinaus stattfinden soll. Bei der ersten Alternative ist dabei unerheblich, ob die Beobachtung ununterbrochen oder in Blöcken von jeweils mehreren Stunden erfolgt. Entscheidend ist allein das Überschreiten der 24-Stunden-Grenze. Bei einer über eine Woche hinausgehenden Observation ist dagegen die Dauer der Beobachtung unbeachtlich. Eine planmäßig angelegte Beobachtung, die - auch mit Unterbrechungen – über eine Woche hinaus andauern soll, wird somit stets von dieser Begriffsbestimmung erfaßt, auch wenn die 24-Stunden-Grenze nicht erreicht wird. Allerdings folgt aus der Formulierung „planmäßig angelegt“, daß ein gelegentliches - auch wiederholtes - kurzfristiges Beobachten, dem keine besonderen Vorbereitungen vorausgehen, nicht von dieser Begriffsbestimmung erfaßt wird.

2

In Absatz 1 Satz 1 Nummern 1 und 2 werden die Voraussetzungen geregelt, unter denen der Einsatz dieser Mittel zulässig ist. Absatz 1 Nummer 1 erlaubt diese Maßnahmen gegenüber Störern im Sinne der §§ 8 und 9 HmbSOG sowie unter den Voraussetzungen des polizeilichen Notstandes (§ 10 HmbSOG) auch gegenüber Nichtverantwortlichen bei einer unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person. Typische Anwendungsfälle hierfür sind Geiselnahmen und Entführungen, bei denen nicht nur Tatverdächtige, sondern auch Dritte - wie z.B. Boten - beobachtet werden müssen. Nach Absatz 1 Nummer 2 ist diese Maßnahme auch zur vorbeugenden Bekämpfung von Straftaten gegenüber potentiellen künftigen Straftätern sowie ihren Kontakt- oder Begleitpersonen zulässig, wenn Tatsachen die Annahme rechtfertigen, daß Straftaten von erheblicher Bedeutung im Sinne des § 1 Absatz 4 begangen werden sollen und der Einsatz zur vorbeugenden Bekämpfung dieser Straftaten erforderlich ist. Eine effektive Strafverfolgung ist - ebenso wie die Verhinderung konkreter Straftaten - nur möglich, wenn die Polizei bereits im Vorfeld einer geplanten Straftat - also auch bevor das Versuchsstadium nach § 22 StGB erreicht wird - Daten erheben kann. Welchen Grad der Wahrscheinlichkeit die Annahme einer drohenden Straftat haben muß, um den Einsatz dieses Mittels zu rechtfertigen, läßt sich nicht generalisieren, sondern nur nach den Umständen des Einzelfalles beantworten. Wie auch bei anderen Prognoseentscheidungen - insbesondere bei der Beurteilung, ob eine allgemeine Gefahr vorliegt - besteht auch hier eine Wechselbeziehung zwischen den der Annahme zugrundeliegenden Tatsachen, der Schwere der drohenden Straftat, der zeitlichen Nähe und der Wahrscheinlichkeit ihrer Begehung. Der besonderen Eingriffsintensität dieser Maßnahme wird im übrigen dadurch Rechnung getragen, daß die Datenerhebung über Kontakt- und Begleitpersonen an die zusätzliche Anforderung geknüpft wird, daß die Aufklärung des Sachverhalts sonst aussichtslos wäre. Absatz 1 Satz 2 berücksichtigt die Tatsache, daß bei den hier gereegelten Mitteln eine Trennung der Personen, gegen die sich die Datenerhebung richtet, von den übrigen Anwesenden nicht immer möglich ist.

3

Wegen ihrer hohen Eingriffsintensität darf die Observation nur vom Polizeipräsidenten angeordnet werden. Insoweit trägt Absatz 2 der Forderung des Bundesverfassungsgerichts nach verfahrensrechtlichen Vorkehrungen zur Sicherung des Rechts auf informationelle Selbstbestimmung Rechnung. Der Inhalt der Anordnung ergibt sich aus den Sätzen 2 und 3. Festzulegen ist insbesondere auch das Ende der Maßnahme. Eine Fortsetzung über das in der Anordnung festgelegte

Ende hinaus ist nur aufgrund einer erneuten Anordnung zulässig, wenn die Voraussetzungen für den Erlaß auch weiterhin bestehen. Die Regelung in Absatz 3 stärkt den effektiven Rechtsschutz des Betroffenen. Danach hat auch im Falle eines sich anschließenden Strafverfahrens in Abstimmung mit der Staatsanwaltschaft eine Unterrichtung des Betroffenen zu erfolgen.

4

Absatz 4 Satz 1 dient zunächst der Klarstellung. Denn daß eine nur kurzfristige Observation nicht von dieser Vorschrift erfaßt werden soll, ergibt sich bereits aus der Begriffsbestimmung in Absatz 1. Auch wenn sie nur über kurze Zeiträume - allenfalls einige Stunden - durchgeführt wird, erreicht sie doch eine gewisse Eingriffsqualität, zumal es sich hierbei im Regelfall um eine verdeckt durchgeführte Maßnahme handelt. Daher ist auch die kurzfristige Observation nur zulässig, wenn sonst die Erfüllung einer polizeilichen Aufgabe gefährdet wäre. Aus der Umschreibung des Anwendungsbereichs dieses Gesetzes in § 1 Absatz 1 ergibt sich, daß diese Maßnahme auch zur Bekämpfung drohender Straftaten zulässig ist, auch wenn diese Straftaten noch keine erhebliche Bedeutung im Sinne von § 1 Absatz 4 aufweisen.

5

Insbesondere für die Bekämpfung des Terrorismus und der Organisierten Kriminalität ist es von entscheidender Bedeutung, daß die Polizei schon im Vorfeld terroristischer und sonstiger Straftaten von erheblicher Bedeutung die Möglichkeiten modernster Ortungs- und Nachrichtentechnologie nutzen kann. Auf diese Weise kann - vom Verdächtigen unbemerkt - ein Bewegungsmuster erstellt werden, um mögliche Komplizen und Hintermänner zu ermitteln. Gerade das Attentat vom 11. September 2001 hat gezeigt, daß terroristische Zellen weltweit und weitgehend im Verborgenen operieren. Absatz 5 stellt den Einsatz von Observationsmethoden wie des sogenannten GPS (Global Positioning System) auf die erforderliche rechtliche Grundlage. Die strafprozessuale Norm des § 100c Absatz 1 Nummer 1b StPO bezeichnet dies als sonstige besondere für Observationszwecke bestimmte technische Mittel. Hierunter fällt auch der Einsatz von GPS. Da die satellitengestützte Ortungsmethode über GPS nicht unter den Begriff der Beobachtung aus § 9 Absatz 1 subsumiert werden kann, mußte die Befugnis um die besonderen für Observationszwecke bestimmten Mittel ergänzt werden.

§ 10 Datenerhebung durch den verdeckten Einsatz technischer Mittel

(1) Die Polizei darf unter den Voraussetzungen von § 9 Absatz 1 Satz 1 Daten erheben durch den verdeckten Einsatz technischer Mittel zur Anfertigung von Bildaufnahmen und Bildaufzeichnungen sowie zum Abhören und Aufzeichnen des gesprochenen Wortes. Der Einsatz unter den Voraussetzungen des § 9 Absatz 1 Satz 1 Nummer 2 ist nur zulässig, wenn Tatsachen die dringende Annahme rechtfertigen, dass die Person Straftaten von erheblicher Bedeutung begehen wird. Die Maßnahme darf auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden. § 9 Absatz 2 gilt entsprechend.

(2) Ein Einsatz nach Absatz 1 zur Datenerhebung in oder aus Wohnungen ist nur unter den Voraussetzungen von § 9 Absatz 1 Satz 1 Nummer 1 zulässig.

(2a) Datenerhebungen nach den Absätzen 1 und 2 sind unzulässig, wenn in ein durch Berufsgeheimnis geschütztes Vertrauensverhältnis im Sinne der §§ 53 und 53a der Strafprozessordnung eingegriffen wird.
(3) In den Fällen des Absatzes 2 darf der Einsatz nur durch den Richter angeordnet werden. Die Anordnung ergeht schriftlich. Sie muss insbesondere Namen und Anschrift des Betroffenen, gegen die sie sich richtet, enthalten und die Wohnung, in oder aus der die Daten erhoben werden sollen, bezeichnen. In ihr sind Art, Umfang und Dauer der Maßnahme zu bestimmen. Sie ist höchstens auf vier Wochen zu befristen. Eine Verlängerung um jeweils nicht mehr als vier Wochen ist zulässig, soweit die in Absatz 2 bezeichneten Voraussetzungen fortbestehen. Bei Gefahr im Verzug kann die Maßnahme durch den Polizeipräsidenten angeordnet werden. Eine richterliche Bestätigung ist unverzüglich einzuholen. Die Maßnahme ist zu beenden, wenn sie nicht innerhalb von drei Tagen von dem Richter bestätigt wird; in diesem Fall sind Bild- und Tonaufzeichnungen unverzüglich zu vernichten, sofern die Aufzeichnungen nicht zur Verfolgung von Straftaten benötigt werden. Zuständig ist das Amtsgericht Hamburg. Das Verfahren richtet sich nach den Vorschriften des Gesetzes über die Angelegenheiten der Freiwilligen Gerichtsbarkeit.
(4) Einer Anordnung nach Absatz 3 und § 9 Absatz 2 Satz 1 bedarf es nicht, wenn technische Mittel ausschließlich zum Schutz der bei einem Polizeieinsatz tätigen Personen mitgeführt und verwendet werden. Der Einsatz in Wohnungen darf nur durch den Leiter des Landeskriminalamtes oder den Polizeiführer vom Dienst angeordnet werden. Eine anderweitige Verwertung der bei einem Einsatz in Wohnungen erlangten Erkenntnisse ist nur zur Abwehr der in § 9 Absatz 1 Satz 1 Nummer 1 genannten Gefahren oder zur Strafverfolgung und nur zulässig, wenn zuvor die Rechtmäßigkeit der Maßnahme richterlich festgestellt ist; bei Gefahr im Verzug ist die richterliche Entscheidung unverzüglich nachzuholen. Aufzeichnungen sind unverzüglich nach Beendigung des Einsatzes zu löschen, es sei denn, sie werden zur Gefahrenabwehr oder Strafverfolgung benötigt.
(5) Die durch eine Maßnahme nach Absatz 2 erlangten personenbezogenen Daten sind besonders zu kennzeichnen. Stellt sich nach Auswertung der Daten heraus, dass diese einem Vertrauensverhältnis zwischen engsten Familienangehörigen oder in gleicher Weise engsten Vertrauten zuzuordnen sind oder keinen unmittelbaren Bezug zu den in Absatz 2 genannten Gefahren haben, dürfen sie nicht verwendet werden, es sei denn, ihre Verwendung ist zur Verhütung einer unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person erforderlich. Die durch eine Maßnahme nach den Absätzen 1 und 2 erlangten Daten, bei denen sich nach Auswertung herausstellt, dass sie einem Vertrauensverhältnis mit Berufsgeheimnisträgern zuzuordnen sind, dürfen nicht verwendet werden.
(6) Personen, gegen die sich die Datenerhebungen richteten oder die von ihr sonst betroffen wurden, sind nach Abschluss der Maßnahme darüber zu unterrichten, sobald dies ohne Gefährdung des Zwecks der Datenerhebung geschehen kann. Erfolgt nach Beendigung einer Maßnahme nach Absatz 2 die Benachrichtigung nicht innerhalb von sechs Monaten, bedarf die weitere Zurückstellung der Benachrichtigung der richterlichen Zustimmung. Entsprechendes gilt nach Ablauf von jeweils weiteren sechs Monaten. Über die Zurückstellung entscheidet das Gericht, das für die Anordnung der Maßnahme

zuständig gewesen ist. § 9 Absatz 3 Satz 2 gilt entsprechend. Eine Unterrichtung kann mit richterlicher Zustimmung unterbleiben, wenn

1. **die Voraussetzungen des Satzes 1 auf Dauer nicht vorliegen oder**
2. **überwiegende schutzwürdige Belange eines Betroffenen entgegenstehen oder**
3. **die Identität oder der Aufenthaltsort eines Betroffenen nur mit unverhältnismäßigem Aufwand ermittelt werden kann.**

(7) Sind die nach Absatz 2 erlangten Daten nicht mehr zur Aufgabenerfüllung erforderlich, sind sie zu löschen. Die Löschung ist zu protokollieren. Die Löschung unterbleibt, soweit die Daten für eine Mitteilung an den Betroffenen nach Absatz 6 oder für eine gerichtliche Nachprüfung der Rechtmäßigkeit der Maßnahme nach Absatz 2 von Bedeutung sein können. In diesem Fall sind die Daten zu sperren und dürfen nur zu diesen Zwecken verarbeitet werden. Im Fall der Unterrichtung des Betroffenen sind die Daten zu löschen, wenn der Betroffene nach Ablauf eines Monats nach seiner Benachrichtigung keine Klage erhebt; auf diese Frist ist in der Benachrichtigung hinzuweisen. Daten, die einem Vertrauensverhältnis zwischen engsten Familienangehörigen oder in gleicher Weise engsten Vertrauten zuzuordnen sind oder keinen unmittelbaren Bezug zu den in Absatz 2 genannten Gefahren haben, sind unverzüglich zu löschen, es sei denn, ihre Verwendung ist zur Verhütung einer unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person erforderlich. Die durch eine Maßnahme nach den Absätzen 1 und 2 erlangten Daten, bei denen sich nach Auswertung herausstellt, dass sie einem Vertrauensverhältnis mit Berufsgeheimnisträgern zuzuordnen sind, sind unverzüglich zu löschen.

(8) Der Senat unterrichtet die Bürgerschaft jährlich über den nach Absatz 2 und, soweit richterlich überprüfungsbedürftig, nach Absatz 4 erfolgten Einsatz technischer Mittel. Ein von der Bürgerschaft gewähltes Gremium übt auf der Grundlage dieses Berichts die parlamentarische Kontrolle aus. Das Gremium besteht aus sieben Mitgliedern der Bürgerschaft. Sie werden in geheimer Abstimmung gewählt.

1

Die Vorschrift regelt die Datenerhebung durch den verdeckten Einsatz technischer Mittel. Ein verdeckter Einsatz liegt vor, wenn das Mittel als solches nicht erkennbar ist. Hierin liegt der Unterschied zur Datenerhebung nach § 8 oder zum offenen Fotografieren einer Person. Ebenfalls nicht erfaßt von dieser Begriffsbestimmung ist der Einsatz von Ferngläsern und ähnlichen Sichthilfen, da hierbei keine Aufzeichnung erfolgt. Die inhaltlichen Voraussetzungen für den Einsatz technischer Mittel entsprechen grundsätzlich denen von § 9. Allerdings ist ein Einsatz zur vorbeugendcn Bekämpfung von Straftaten nur zulässig, wenn Tatsachen die dringende Annahme rechtfertigen, daß die Zielperson Straftaten von erheblicher Bedeutung begehen wird. Die „dringende Annahme“ hat dabei eine ähnliche Bedeutung wie der dringende Tatverdacht im Strafverfahrensrecht. Erforderlich ist somit eine große oder überwiegende Wahrscheinlichkeit. Eine an Sicherheit grenzende Wahrscheinlichkeit wird dagegen nicht vorausgesetzt.

2

Die Regelungen in § 10 tragen den Ausführungen des Bundesverfassungsgerichts in seinen Entscheidungen vom 3. März 2004 (Urteil zur repressiven Wohnraumüberwachung - 1 BvR 2378/98 - und Beschluss zur präventiven Telekommunikationsüberwachung nach dem Außenwirtschaftsgesetz - 1 BvF 3/92 -) Rechnung. In seinem Urteil hat das Bundesverfassungsgericht das Instrument der Wohnraumüberwachung grundsätzlich für verfassungsgemäß erklärt. Es hat jedoch festgestellt, daß in den absolut geschützten Kernbereich privater Lebensgestaltung als Ausprägung der Unantastbarkeit der Menschenwürde gemäß Artikel 1 Absatz 1 des Grundgesetzes zu Strafverfolgungszwecken nicht eingegriffen werden darf. Eine unmittelbare Übertragung der im Urteil des Bundesverfassungsgerichts zur repressiven Wohnraumüberwachung dargelegten Grundsätze auf die in Absatz 2 geregelte präventive Wohnraumüberwachung scheidet wegen der unterschiedlichen Zwecke der Maßnahmen aus. Während die strafprozessuale Maßnahme dem staatlichen Strafanspruch und letztlich dem Allgemeininteresse an der Wiederherstellung des durch die Straftat gestörten Rechtsfriedens dient, erfolgt die präventive Maßnahme zum Schutz einer Person, von der eine Gefahr für Leib, Leben oder Freiheit abgewendet werden soll. Soweit also der Störer selbst in schutzwürdige Sphären Dritter eingreift, kann er sich nicht auf einen unantastbaren Kernbereich privater Lebensgestaltung berufen. Auch bedürfen die geschützten Rechtsgüter keiner weiteren Einschränkung, denn die präventive Wohnraumüberwachung ist nur zum Schutz hochwertigster Rechtsgüter zulässig. Aus diesem Grund ist schließlich auch keine Regelung erforderlich, die zum einen die Maßnahme nur zulässt, wenn die Annahme gerechtfertigt erscheint, daß die Gespräche einen Bezug zur Gefahr aufweisen, oder zum anderen eine Unterbrechung der Maßnahme für den Fall anordnet, daß der Kernbereich privater Lebensgestaltung berührt ist. Bei einer derartigen Gefahrenlage würden Aufklärungsmaßnahmen im Vorfeld einen zu großen Zeitverlust verursachen und Unterbrechungen die Gefahr herbeiführen, daß für den Schutz des Opfers entscheidende Informationen nicht erhoben werden. Der Schutz vor einer unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit überwiegt insoweit den Schutz des Kernbereichs privater Lebensgestaltung. Zwar ist es nach den Maßstäben des Bundesverfassungsgerichts nicht zwingend geboten, die Vertrauensverhältnisse mit sämtlichen Berufsgeheimnisträgern und ihren Berufshelfern von einer Überwachung auszunehmen. Gleichwohl werden aus rechtpolitischen Erwägungen in Absatz 2a Eingriffe in durch Berufsgeheimnis geschützte Vertrauensverhältnisse nach den §§ 53 und 53a StPO für unzulässig erklärt. Entsprechende Sonderregelungen enthalten auch die Verwendungs- und Löschungsvorschriften in Absatz 5 und 7. Das Urteil ist hinsichtlich der vom Bundesverfassungsgericht geforderten verfahrenssichernden Maßnahmen auch bei der präventiven Wohnraumüberwachung zu berücksichtigen. Verfahrenssichernde Maßnahmen stellen bei einer polizeilichen Datenerhebung aus verfassungsrechtlich geschützten Vertrauensverhältnissen einen Ausgleich zwischen den konkurrierenden Rechtspositionen her und dienen der Gewährleistung der betroffenen Grundrechte. So enthält Absatz 3 eine konkretere Ausgestaltung des Richtervorbehalts, mit der die inhaltlichen Anforderungen an die richterliche Anordnung präzisiert werden. Danach sind in der Anforderung Art und Weise sowie Dauer und Umfang der Maßnahme schriftlich zu bestimmen.

3

In Absatz 5 werden das Kennzeichnungsgebot und die Verwendungsbeschränkungen geregelt. Die Kennzeichnung der aus der Wohnraumüberwachung stammenden Daten dient der Gewährung der Zweckbindung, da auf diese Weise nach der Informationserhebung erkennbar bleibt, daß es sich um entsprechend sensible Daten handelt. Einem Verwendungsverbot unterliegen hingegen Daten, die keinen Bezug zu der abzuwehrenden Gefahr aufweisen oder bei denen sich nachträglich herausstellt, daß in ein besonderes Vertrauensverhältnis eingegriffen wurde. Eine Ausnahme hiervon besteht wiederum für Daten, die zum Schutz anderer hochwertigster Rechtsgüter erforderlich sind. Die Unterrichtungsvorschriften in Absatz 6 dienen insbesondere der verbesserten Wahrnehmung effektiven Rechtsschutzes. Die Zurückstellung der Benachrichtigung bedarf jeweils nach sechs Monaten der richterlichen Zustimmung. In den besonders aufgeführten Fallkonstellationen kann mit richterlicher Zustimmung eine Benachrichtigung auch auf Dauer unterbleiben. Die besonderen Löschungsregelungen in Absatz 7 sollen insbesondere den von der Maßnahme betroffenen Personen die nachträgliche Inanspruchnahme von Rechtsschutz ermöglichen. Die Daten werden insoweit zunächst gesperrt. Eine sofortige Löschung ist nur dann zwingend geboten, wenn die Datenerhebung den Kernbereich privater Lebensgestaltung berührt hat, da die weitere Aufbewahrung dieser Daten zu einer unverhältnismäßigen Vertiefung dieser Rechtsverletzung führen würde. Eine Ausnahme hiervon besteht wiederum für Daten, die zum Schutz anderer hochwertigster Rechtsgüter erforderlich sind.

§ 10a Datenerhebung durch Telekommunikationsüberwachung und Eingriff in die Telekommunikation

(1) Die Polizei darf Daten erheben durch die Überwachung und Aufzeichnung von Telekommunikation einschließlich der innerhalb des Telekommunikationsnetzes in Datenspeichern abgelegten Inhalte

1. **über die für eine Gefahr Verantwortlichen und unter den Voraussetzungen des §10 SOG über die dort genannten Personen, wenn dies zur Abwehr einer unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist,**
2. **über Personen, soweit Tatsachen die Annahme rechtfertigen, dass diese Personen besonders schwerwiegende Straftaten begehen werden, wenn die Datenerhebung zur vorbeugenden Bekämpfung von Straftaten erforderlich ist, sowie**
3. **über deren Kontakt- und Begleitpersonen, wenn die Aufklärung des Sachverhaltes auf andere Weise aussichtslos wäre.**

Die Maßnahme darf auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden. Datenerhebungen sind unzulässig, wenn in ein durch Berufsgeheimnis geschütztes Vertrauensverhältnis im Sinne der §§ 53 und 53 a der Strafprozessordnung eingegriffen wird.

(2) Besonders schwerwiegende Straftaten im Sinne des Absatzes 1 sind

1. **Straftaten des Friedensverrats, des Hochverrats und der Gefährdung des demokratischen Rechtsstaates oder des Landesverrats und der Gefährdung der äußeren Sicherheit (§§ 80, 81, 82, 94, § 96 Absatz 1, jeweils auch in Verbindung mit §§ 97a, 97b, § 98 Absatz 1 Satz 2, § 99 Absatz 2, § 100, § 100a Absatz 4 des Strafgesetzbuches),**

2. Straftaten gegen die öffentliche Ordnung (§§ 129 bis 130 des Strafgesetzbuches, § 95 Absatz 1 Nummer 8 des Aufenthaltsgesetzes),
3. Straftaten gegen die sexuelle Selbstbestimmung (§§ 176, 176a, 177, 180b, 181, § 181a Absatz 1 des Strafgesetzbuches),
4. Straftaten gegen das Leben (§§ 211, 212 des Strafgesetzbuches, § 6 des Völkerstrafgesetzbuches),
5. Straftaten gegen die persönliche Freiheit (§ 234, § 234a Absatz 1, §§ 239a, 239 b des Strafgesetzbuches),
6. Straftaten nach § 244 Absatz 1 Nummer 2, §§ 244a, 249 bis 251, 253, 255, 260, 260a des Strafgesetzbuches,
7. gemeingefährliche Straftaten in den Fällen der §§ 306 bis 306b, § 307 Absatz 1 und 2, § 308 Absatz 1, § 309 Absatz 1, § 310 Absatz 1, §§ 313, 314, § 315 Absatz 3, § 315b Absatz 3, §§ 316a, 316c des Strafgesetzbuches),
8. Verbrechen gegen die Menschlichkeit (§ 7 des Völkerstrafgesetzbuches),
9. Straftaten nach § 51 Absatz 1 in Verbindung mit Absatz 2, § 52 Absatz 1 Nummer 1 in Verbindung mit Absatz 5 des Waffengesetzes oder nach § 19 Absatz 2, § 20 Absatz 1, jeweils auch in Verbindung mit § 21 des Gesetzes über die Kontrolle von Kriegswaffen,
10. Straftaten nach § 22a Absatz 1 in Verbindung mit Absatz 2 des Gesetzes über die Kontrolle von Kriegswaffen,
11. Straftaten nach einer in § 29 Absatz 3 Satz 2 Nummer 1 des Betäubungsmittelgesetzes in Bezug genommenen Vorschrift unter den dort genannten Voraussetzungen oder nach § 29a, § 30 Absatz 1 Nummern 1, 2, 4, §§ 30a und 30b des Betäubungsmittelgesetzes und
12. Straftaten nach § 96 Absatz 2 und § 97 des Aufenthaltsgesetzes oder nach § 84 Absatz 3 und § 84a des Asylverfahrensgesetzes.

(3) Durch den Einsatz technischer Mittel dürfen unter den Voraussetzungen des Absatzes 1 Satz 1 Nummern 1 und 2 Kommunikationsverbindungen unterbrochen oder verhindert werden. Kommunikationsverbindungen Dritter dürfen nur unterbrochen oder verhindert werden, wenn dies zur Abwehr einer unmittelbar bevorstehenden erheblichen Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person erforderlich ist.

(4) Auf Grund der Anordnung einer Datenerhebung nach Absatz 1 hat jeder, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt (Diensteanbieter), nach Maßgabe der Regelungen des Telekommunikations-gesetzes und der darauf beruhenden Rechtsverordnungen zur technischen und organisatorischen Umsetzung von Überwachungsmaßnahmen der Polizei die Überwachung, Aufzeichnung und Unterbrechung von Telekommunikations-verbindungen zu ermöglichen.

1

Absatz 1 regelt die Telekommunikationsüberwachung und -aufzeichnung. Der Begriff Telekommunikation ist definiert in § 3 Nummer 22 des Telekommunikationsgesetzes (BGBl. I 2004, S. 1190). Danach ist Telekommunikation der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunika-tionsanlagen. Für die polizeiliche Gefahrenabwehr sind drei Bereiche von besonderer Bedeutung. Zum einen kann die Polizei Gespräche zwischen zwei Personen überwachen. Eine solche Maßnahme richtet sich in erster Linie auf den

Gesprächsinhalt. Gleichzeitig werden bei dieser Überwachung aber auch automatisch Verkehrsdaten an die Polizei übermittelt. Die Ermittler erhalten so genaue Informationen über den Inhaber des Anschlusses. Zum anderen können auch Mailboxen überprüft werden, die in einem Datenspeicher innerhalb des Telekommunikationsnetzes abgelegt werden. Ein dritter Bereich der Telekommunikationsüberwachung ist die Ortung eines Mobilfunktelefons. Das Mobilfunktelefon nimmt automatisch Verbindung zu der nächstgelegenen Funkzelle auf. Bei der Überwachung eines Mobilfunktelefons wird daher immer auch der Standort des Benutzers übermittelt. Dies gilt für den Fall, daß mit dem Mobilfunktelefon ein Gespräch geführt wird, als auch für den Fall, daß das Mobilfunktelefon sich lediglich im Stand-By Modus befindet. In den Nummern 1 bis 3 werden die Voraussetzungen geregelt, unter denen der Einsatz dieser Mittel zulässig ist. Der Adressatenkreis orientiert sich an der Regelung in § 9 Absatz 1. Die Überwachungsmaßnahmen dürfen nach Nummer 1 gegenüber Störern im Sinne der §§ 8 und 9 HmbSOG und unter den Voraussetzungen des § 10 HmbSOG auch gegenüber Nicht-Störern im Rahmen der Notstandshaftung zur Abwehr einer Gefahr für die abschließend aufgezählten Rechtsgüter durchgeführt werden. Die Maßnahme kann darüber hinaus nach Nummer 2 zur vorbeugenden Bekämpfung von besonders schwerwiegenden Straften zur Anwendung gelangen. Die Regelung trägt den besonderen Erfordernissen der Vorfeldermittlung mit dem Ziel des Erkennens krimineller Strukturen Rechnung. Es müssen jedoch bereits überprüfbare Anhaltspunkte dafür vorliegen, daß die Personen entsprechende Straftaten begehen werden. Nummer 3 schließlich erfaßt auch die Kontakt- und Begleitpersonen, bei denen allerdings strengere Voraussetzungen vorliegen müssen. Die Heranziehung von Unbeteiligten hat danach immer nur nachrangig zu erfolgen, wenn andere Maßnahmen - insbesondere gegenüber den unter Nummer 2 genannten Personen - nicht in Betracht kommen und ohne die Einbeziehung der Kontakt- und Begleitpersonen die Verhinderung der bevorstehenden Straftat nicht möglich erscheint. Nach Absatz 1 Satz 3 sind Datenerhebungen unzulässig, die in ein durch Berufsgeheimnis geschütztes Vertrauensverhältnis eingreifen.

2

Absatz 2 definiert die in Absatz 1 Satz 1 Nummer 2 als Eingriffsvoraussetzung normierten besonders schwerwiegenden Straftaten. Die im Vergleich zu den verdeckten Maßnahmen der Observation und des Einsatzes verdeckter Ermittler höhere Eingriffsintensität der Telekommunikationsüberwachung macht es erforderlich, einen von den Straftaten von erheblicher Bedeutung im Sinne von § 1 Absatz 4 abgesetzten Katalog von besonders schwerwiegenden Straftaten zu normieren, zu deren Verhütung die Telekommunikationsüberwachung eingesetzt werden kann. Die enumerative und abschließende Aufzählung der Straftaten trägt gleichzeitig dem Beschluß des Bundesverfassungsgerichts vom 3. März 2004 (1 BvF 3/92) Rechnung. Das Bundesverfassungsgericht hat dort den Anforderungen an die Normenbestimmtheit und Normenklarheit der Ermächtigungen zum Eingriff in das Grundrecht aus Artikel 10 Absatz 1 GG im Bereich der Straftatenverhütung ein besonders hohes Gewicht beigemessen. Der Katalog orientiert sich im wesentlichen an den vom Bundesverfassungsgericht im Urteil zur repressiven Wohnraumüberwachung aufgestellten Kriterien. Ein ausschließliches Abstellen auf das Strafmaß - und zwar auf eine Höchststrafe von mehr als fünf Jahren - ist nicht geboten, denn Artikel 10 GG enthält im Gegensatz zu Artikel 13 Absatz 3 GG nicht die einengende Eingriffsvoraussetzung des Verdachts einer besonders schweren Straftat. Darüber hinaus sind bei gefahrenabwehrenden Maßnahmen insbesondere

die Gefahren für die öffentliche Sicherheit, die von bestimmten Straftaten ausgehen, zu berücksichtigen.

3

Eine Rechtsgrundlage für die Verbindungsunterbrechung bzw. -verhinderung wird in Absatz 3 Satz 1 geschaffen. Mit dieser Maßnahme sollen Telekommunikationsverbindungen der in Absatz 1 Nummer 1 und 2 genannten Störer oder potentieller Straftäter unterbrochen oder künftige Verbindungen von oder zu den Genannten verhindert werden. So haben gerade die Anschläge in Madrid im März 2004 gezeigt, daß über ein Mobiltelefon der Zündmechanismus für eine Bombe ausgelöst werden kann. Darüber hinaus kann potentiellen Straftätern die Planung und Koordination ihres Vorhabens erheblich erschwert werden. Die Polizei kann so die notwendige Zeit gewinnen, um anderweitige Maßnahmen zu ergreifen, mittels derer die Gefahr endgültig beseitigt werden kann. Absatz 3 Satz 2 ermöglicht eine solche Maßnahme auch gegenüber Dritten. Wegen des erheblichen Grundrechtseingriffs ist dies nur zulässig zur Abwehr von Gefahren für Rechtsgüter von überragender Bedeutung.

4

Absatz 4 regelt die Mitwirkungspflichten derjenigen, die geschäftsmäßig Telekommunikationsdienste anbieten, erbringen oder daran mitwirken (Dienstanbieter). Für die Telekommunikationsüberwachung und -aufzeichnung ergibt sich das durch den Verweis auf das Telekommunikationsgesetz. Dort ist detailliert geregelt, auf welche Weise die Anbieter verpflichtet sind, der Polizei zu helfen. Die Mitwirkungspflicht erstreckt sich auch auf solche Diensteanbieter, deren Firmensitz außerhalb Hamburgs liegt, sofern sie ihre Dienste auch in Hamburg anbieten.

§ 10b Verkehrsdatenerhebung und Einsatz besonderer technischer Mittel zur Datenerhebung

(1) Die Polizei darf unter den Voraussetzungen des § 10a Absatz 1 Daten erheben durch Auskünfte über Telekommunikationsverbindungen.

(2) Die Erteilung einer Auskunft darüber, ob von einem Telekommunikationsanschluss Telekommunikationsverbindungen zu den in § 10a Absatz 1 genannten Personen hergestellt worden sind (Zielsuchlauf), darf nur angeordnet werden, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos wäre.

(3) Durch den Einsatz technischer Mittel darf

1. **zur Vorbereitung einer Maßnahme nach § 10a Absatz 1 die Geräte- und Kartennummer,**
2. **zur Abwehr einer unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit der Standort eines aktiv geschalteten Mobilfunkendgerätes ermittelt werden.**

Die Maßnahme nach Satz 1 Nummer 1 ist nur zulässig, wenn die Voraussetzungen des § 10a Absatz 1 vorliegen und die Durchführung der Überwachungsmaßnahme ohne die Geräte- und Kartennummer nicht möglich oder wesentlich erschwert wäre. Die Maßnahme nach Satz 1 Nummer 2 ist nur dann zulässig, wenn die Ermittlung des Aufenthaltsortes auf andere Weise weniger Erfolg versprechend oder erschwert wäre. Personenbezogene Daten Dritter dürfen anlässlich solcher Maßnahmen nur erhoben werden, wenn dies

aus technischen Gründen zur Erreichung des Zwecks nach Absatz 1 unvermeidbar ist.
(4) Jeder Diensteanbieter ist verpflichtet, der Polizei auf Grund der Anordnung einer Datenerhebung nach Absatz 1
1. **vorhandene Telekommunikationsdaten zu übermitteln,**
2. **Daten über zukünftige Telekommunikationsverbindungen zu übermitteln oder**
3. **die für die Ermittlung des Standortes eines Mobilfunkendgerätes nach Absatz 3 erforderlichen spezifischen Kennungen, insbesondere die Geräte- und Kartennummer mitzuteilen.**

Die Daten sind der Polizei unverzüglich oder innerhalb der in der Anordnung bestimmten Zeitspanne sowie auf dem darin bestimmten Übermittlungsweg zu übermitteln.
(5) Verkehrsdaten sind alle nicht inhaltsbezogenen Daten, die im Zusammenhang mit einer Telekommunikation auch unabhängig von einer konkreten Telekommunikationsverbindung technisch erhoben und erfasst werden, insbesondere
1. **Berechtigungskennung, Kartennummer, Standortkennung sowie Rufnummer oder Kennung des anrufenden und angerufenen Anschlusses oder der Endeinrichtung,**
2. **Beginn und Ende der Verbindung nach Datum und Uhrzeit,**
3. **vom Kunden in Anspruch genommene Telekommunikationsdienstleistung,**
4. **Endpunkte fest geschalteter Verbindungen, ihr Beginn und Ende nach Datum und Uhrzeit.**

1

In dieser Vorschrift wird die Verkehrsdatenabfrage geregelt. Sie bezieht sich in erster Linie auf bereits erfolgte Gespräche. Es wird damit bei einer Maßnahme nach § 10b keine aktuell bestehende Telekommunikationsverbindung erfaßt. Vielmehr können die Ermittler in Erfahrung bringen, welche Telekommunikationsverbindungen von einem bestimmten Anschluss hergestellt wurden. Gleiches gilt auch für versandte E-Mails. So kann zwar nicht mehr der Inhalt der Telekommunikationsverbindung ermittelt werden, wohl aber ihr Verlauf. Es können anhand solcher Erkenntnisse Beziehungsnetze und Strukturen von terroristischen Vereinigungen oder der Organisierten Kriminalität aufgedeckt werden.

2

Eine besondere Form der Verkehrsdatenabfrage ist in Absatz 2 geregelt. Es handelt sich um den sogenannten Zielsuchlauf (Umkehrsuche). Ausgangspunkt des Zielsuchlaufs sind nicht die Verbindungen, welche von dem überprüften Anschluss aufgebaut wurden, sondern die Anschlüsse, welche von sich aus eine Verbindung mit dem überprüften Anschluss aufgebaut haben. Die Regelung in Absatz 3 ermöglicht den Einsatz von so genannten „IMSI-Catchern“ auch für polizeilich-präventive Zwecke. Die Erfahrungen aus der Polizeipraxis zeigen die Notwendigkeit der Identifizierung und Standortbestimmung von Mobiltelefonen zur Vorbereitung von Überwachungsmaßnahmen nach § 10a Absatz 1 sowie zur Abwehr unmittelbar bevorstehender Gefahren für Leib, Leben und Freiheit.

3

Absatz 3 entspricht in seiner Struktur dem durch das Gesetz zur Änderung der Strafprozeßordnung vom 6. August 2002 (BGBl. I S. 3018) neu eingeführten § 100i StPO. Er schafft die rechtliche Grundlage für den polizeilich-präventiven Einsatz spezieller Messgeräte (sog. „IMSI-Catcher“) zur Identifizierung von Geräte- und Kartennummer sowie zur Standortbestimmung von Mobiltelefonen. Die Notwendigkeit der Identifizierung von Gerätenummer und Kennung eines Mobiltelefons (Absatz 3 Nummer 1) ergibt sich aus der Tatsache, daß im Bereich der Organisierten Kriminalität zunehmend Mobiltelefone benutzt werden, deren Herkunft nicht bekannt ist, so daß auch die Rufnummer nicht zu ermitteln ist. Für die Anordnung einer Überwachungsmaßnahme nach § 10a Absatz 1 ist aber die Rufnummer oder eine andere Kennung des Telekommunikationsanschlusses zwingend erforderlich, so daß eine Abhörmaßnahme gemäß § 10a Absatz 1 in diesen Fällen ausscheiden würde. Daher wird zur Abwehr einer unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit bzw. zur vorbeugenden Verhinderung von besonders schwerwiegenden Straftaten die Identifizierung der Gerätenummer zur Vorbereitung einer Maßnahme nach § 10a Absatz 1 benötigt. Die Maßnahmen nach Absatz 3 Nummer 2 dürfen nur zur Abwehr einer unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit erfolgen, nicht jedoch zur vorbeugenden Bekämpfung von besonders schwerwiegenden Straftaten. Hieran zeigt sich die strikt am rechtsstaatlichen Verhältnismäßigkeitsprinzip orientierte Eingriffsgrundlage, die wesentlich restriktiver ist als bei Abhörmaßnahmen gemäß § 10a Absatz 1. Die Rechtsgüterabwägung zwischen den Grundrechten der Betroffenen (Störer und Nichtstörer) einerseits und dem öffentlichen Interesse (Schutz von Leben und Gesundheit, Artikel 2 Absatz 2 GG) andererseits ergibt einen Vorrang für die Durchführung der schwerwiegenden Maßnahme im öffentlichen Interesse. Die Polizei hat die verfassungsrechtliche Schutzpflicht für das Leben und die Gesundheit der Bürger aus Artikel 2 Absatz 2 GG wahrzunehmen. Diese wichtigsten Rechtsgüter überwiegen die nur vorübergehend eingeschränkten Grundrechte des Fernmeldegeheimnisses und des informationellen Selbstbestimmungsrechts. Die polizeilichen Erfahrungen mit telefonisch angekündigten Suizidabsichten zeigen, daß eine schnelle Standortbestimmung gemäß Absatz 3 Nummer 2 unerlässlich ist, um den Suizidgefährdeten von seiner Tat abzuhalten. Gleiches gilt für die Ortung hilfloser Personen, die verunglückt sind und sich nicht mehr über ihren genauen Standort äußern können. In solchen Fallkonstellationen kann nur eine unverzügliche polizeiliche Standortbestimmung mittels eines „IMSI-Catchers“ das Auffinden der hilflosen und oftmals schwer verletzten Person ermöglichen und die Einleitung von Rettungsmaßnahmen gewährleisten.

4

Absatz 4 regelt die Übermittlung der in Absatz 5 einzeln aufgeführten Verbindungsdaten durch die Diensteanbieter. Es handelt sich vor allem um Teilnehmerkennungen, Beginn und Ende von Verbindungen einschließlich Datum und Uhrzeit sowie Positionsmeldungen. Die Legaldefinition orientiert sich an § 96 Telekommunikationsgesetz; im Hinblick auf weitere zu erwartende technische Entwicklungen wird auf eine abschließende Aufzählung verzichtet. Die Anordnung zur Übermittlung ist auch für erst in der Zukunft anfallende Verbindungsdaten zulässig. Damit ist zugleich die Verpflichtung zur Aufzeichnung dieser Daten umfaßt. Die Inanspruchnahme der Diensteanbieter erfolgt sowohl aus besonderer Sachnähe

als auch aus einem besonderen Pflichtenverhältnis heraus, das sie - wie den §§ 111 ff TKG zu entnehmen ist - gegenüber den Sicherheitsbehörden zur Bereitstellung von Daten verpflichtet.

§ 10c Anordnung und Ausführung

(1) Maßnahmen nach §§ 10a und 10b bedürfen einer Anordnung durch einen Richter. Bei Gefahr im Verzug kann die Maßnahme durch den Polizeipräsidenten angeordnet werden. Eine richterliche Bestätigung ist unverzüglich einzuholen. Die Maßnahme ist zu beenden, wenn sie nicht innerhalb von drei Tagen von einem Richter bestätigt wird; in diesem Fall sind die Datenaufzeichnungen unverzüglich zu vernichten, wenn diese nicht zur Strafverfolgung benötigt werden. Zuständig ist das Amtsgericht Hamburg. Das Verfahren richtet sich nach den Vorschriften des Gesetzes über die Angelegenheiten der Freiwilligen Gerichtsbarkeit.

(2) Die Anordnung nach §§ 10a und 10b muss den Namen und die Anschrift des Betroffenen, gegen den sie sich richtet, sowie die Rufnummer oder eine andere Kennung seines Telekommunikationsanschlusses enthalten. Sofern andernfalls die Erreichung des Zwecks aussichtslos oder erheblich erschwert wäre, genügt eine räumlich und zeitlich hinreichende Bezeichnung der Telekommunikation, über die personenbezogene Daten erhoben oder über die Auskunft erteilt werden soll; dies gilt nicht für Maßnahmen nach § 10a Absatz 1 Satz 1 Nummer 3. Die Anordnung nach § 10a Absatz 1 und § 10b Absatz 2 ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei Monate ist zulässig, wenn die Voraussetzungen für die Maßnahme noch vorliegen. Die Anordnung nach § 10a Absatz 3 Satz 1 ist auf höchstens zwei Wochen und die Anordnung nach § 10a Absatz 3 Satz 2 auf höchstens zwei Tage zu befristen.

(3) Die durch eine Maßnahme nach §§ 10a und 10b erlangten Daten sind besonders zu kennzeichnen. Sie dürfen für einen anderen Zweck verwendet werden, soweit dies zur Abwehr einer unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit, zur vorbeugenden Bekämpfung einer besonders schwerwiegenden Straftat oder zur Verfolgung von besonders schwerwiegenden Straftaten erforderlich ist. Die Daten, welche auf Grund einer Maßnahme nach § 10b Absatz 2 erlangt werden, dürfen über den Datenabgleich zur Ermittlung der gesuchten Geräte- und Kartennummer hinaus nicht verwendet werden. Daten, bei denen sich nach Auswertung herausstellt, dass sie einem Vertrauensverhältnis zwischen engsten Familienangehörigen oder in gleicher Weise engsten Vertrauten zuzuordnen sind oder keinen unmittelbaren Bezug zu den in § 10a Absatz 1 genannten Gefahren oder Straftaten haben, dürfen nicht verwendet werden, es sei denn, ihre Verwendung ist zur Verhütung einer unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person erforderlich. Daten, bei denen sich nach Auswertung herausstellt, dass sie einem Vertrauensverhältnis mit Berufsgeheimnisträgern zuzuordnen sind, dürfen nicht verwendet werden.

(4) Personen, gegen die sich die Datenerhebungen nach §§ 10a oder 10b richteten oder die von ihr sonst betroffen wurden, sind nach Abschluss der Maßnahme darüber zu unterrichten, sobald dies ohne Gefährdung des Zwecks der Datenerhebung geschehen kann. Erfolgt nach Beendigung einer Maßnahme die Benachrichtigung nicht innerhalb von sechs Monaten, bedarf

die weitere Zurückstellung der Benachrichtigung der richterlichen Zustimmung. Entsprechendes gilt nach Ablauf von jeweils weiteren sechs Monaten. Über die Zurückstellung entscheidet das Gericht, das für die Anordnung der Maßnahme zuständig gewesen ist. § 9 Absatz 3 Satz 2 und § 10 Absatz 6 Satz 6 gelten entsprechend.
(5) Sind die nach §§ 10a oder 10b erlangten Daten zur Aufgabenerfüllung nicht mehr erforderlich, sind sie zu löschen. Die Löschung ist zu protokollieren. Die Löschung unterbleibt, soweit die Daten für eine Mitteilung an den Betroffenen nach Absatz 4 oder für eine gerichtliche Nachprüfung der Rechtmäßigkeit der Maßnahme von Bedeutung sein können. In diesem Fall sind die Daten zu sperren und dürfen nur zu diesen Zwecken verarbeitet werden. § 10 Absatz 7 Satz 5 gilt entsprechend. Daten, die einem Vertrauensverhältnis zwischen engsten Familienangehörigen oder in gleicher Weise engsten Vertrauten zuzuordnen sind oder keinen unmittelbaren Bezug zu den in § 10a Absatz 1 genannten Gefahren oder Straftaten haben, sind unverzüglich zu löschen, es sei denn, ihre Verwendung ist zur Verhütung einer unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person erforderlich. Daten, bei denen sich nach Auswertung herausstellt, dass sie einem Vertrauensverhältnis mit Berufsgeheimnisträgern zuzuordnen sind, sind unverzüglich zu löschen.

1

Die Vorschrift regelt die verfahrensrechtlichen Anforderungen. Die Maßnahmen nach § 10a Absatz 1 und § 10b stehen danach wegen der hohen Bedeutung des Fernmeldegeheimnisses unter einem richterlichen Anordnungsvorbehalt. Nur in Ausnahmefällen, nämlich bei Gefahr im Verzug, darf die Maßnahme durch den Polizeipräsidenten angeordnet werden. In einem solchen Fall muß innerhalb von drei Tagen eine Bestätigung eines Richters eingeholt werden. Zuständig ist das Amtsgericht Hamburg. Wird die Maßnahme nicht binnen drei Tagen richterlich bestätigt, so sind die erlangten Daten sofort zu löschen, sofern sie nicht zu Zwecken der Strafverfolgung benötigt werden.

2

Nach Absatz 2 ist die Anordnung in schriftlicher Form zu erlassen und hat in der Regel die genaue Bezeichnung des Betroffenen sowie die Angabe der Rufnummer oder einer anderen Kennung zu enthalten. Nur in den Fällen, in denen die Zweckerreichung sonst aussichtslos oder erheblich erschwert wäre, kann zum Beispiel die namentliche Identifizierung des Betroffenen durch eine räumlich und zeitlich hinreichend genaue Bezeichnung der zu überwachenden Telekommunikation ersetzt werden. So müssen etwa die von einer Telekommunikationsunterbrechung oder -verhinderung betroffenen Personen lediglich räumlich genau bezeichnet werden. Die Regelungen über die Befristung orientieren sich im wesentlichen an den entsprechenden Regelungen zu Telekommunikationsüberwachungsmaßnahmen im strafprozessualen Bereich und betragen einheitlich drei Monate mit einer Verlängerungsmöglichkeit von weiteren drei Monaten unter der Bedingung, daß die Voraussetzungen weiterhin vorliegen. Hinsichtlich der Maßnahme der Telekommunikationsunterbrechung und -verhinderung wird wegen der erheblichen Eingriffsintensität eine deutlich geringere Frist von zwei Wochen bzw. zwei Tagen festgesetzt.

3

Absätze 3 bis 5 regeln besondere verfahrenssichernde Maßnahmen. Es handelt sich um Kennzeichnungs-, Zweckänderungs-, Unterrichtungs- und Löschungsregelungen. Es gelten die Ausführungen zu § 10 Absätze 5 bis 7 entsprechend. Im Unterschied zur Wohnraumüberwachung dürfen die erlangten Daten zur Strafverfolgung, aber nur zur Verfolgung von besonders schwerwiegenden Straftaten verwendet werden.

§ 11 Datenerhebung durch den Einsatz von Personen, deren Zusammenarbeit mit der Polizei Dritten nicht bekannt ist

(1) Die Polizei darf unter den Voraussetzungen von § 9 Absatz 1 Satz 1 Daten erheben durch den Einsatz von Personen, deren Zusammenarbeit mit der Polizei Dritten nicht bekannt ist. Die Maßnahme darf auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.

(2) § 9 Absätze 2 und 3 gilt entsprechend. Eine Unterrichtung kann auch unterbleiben, wenn hierdurch der weitere Einsatz dieser Person oder Leib oder Leben einer Person gefährdet wird.

Einen Einsatz nach dieser Bestimmung setzt den gezielten Auftrag an eine Vertrauensperson voraus, personenbezogene Daten zu einem bestimmten Sachverhalt oder über eine bestimmte Person zu beschaffen. Hierunter fällt somit nicht das gezielte Befragen von Zeugen und Hinweisgebern nach bestimmten Tatsachen oder eine allgemeine Bitte an bestimmte Personen, ihr sachdienliche Hinweise über verdächtige Sachverhalte zu geben, die jeweils als Datenerhebung bei Dritten unter den Voraussetzungen von § 6 in Verbindung mit § 2 Absatz 2 zulässig ist. Erst durch die gezielte Zusammenarbeit mit der Vertrauensperson erhält diese Maßnahme eine besondere Eingriffsqualität. Zulässig ist der Einsatz von Vertrauenspersonen unter den Voraussetzungen des § 9. Die weitergehende Beschränkung bezüglich der Benachrichtigung der vom Einsatz betroffenen Personen nach Absatz 2 trägt den Besonderheiten bei dieser Form der Datenerhebung Rechnung.

§ 12 Datenerhebung durch den Einsatz Verdeckter Ermittler

(1) Die Polizei darf durch einen Vollzugsbeamten, der unter einer ihm verliehenen, auf Dauer angelegten, veränderten Identität (Legende) eingesetzt wird (Verdeckte Ermittler), personenbezogene Daten über die für eine Gefahr verantwortlichen und andere Personen erheben, wenn

1. **dies zur Abwehr einer unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist,**
2. **Tatsachen die Annahme rechtfertigen, dass Straftaten von erheblicher Bedeutung begangen werden sollen und der Einsatz zur vorbeugenden Bekämpfung dieser Straftaten erforderlich ist; der gezielte Einsatz gegen bestimmte Personen ist nur zulässig, wenn Tatsachen die dringende Annahme rechtfertigen, dass diese Personen Straftaten von erheblicher Bedeutung begehen werden und die Aufklärung des Sachverhalts auf andere Weise aussichtslos wäre.**

Der Einsatz bedarf außer bei Gefahr im Verzuge der Zustimmung der Staatsanwaltschaft.

(2) Soweit es für den Aufbau und zur Aufrechterhaltung der Legende unerlässlich ist, dürfen entsprechende Urkunden hergestellt oder verändert werden. Ein Verdeckter Ermittler darf zur Erfüllung seines Auftrages unter der Legende am Rechtsverkehr teilnehmen.
(3) Ein Verdeckter Ermittler darf unter der Legende mit Einverständnis des Berechtigten dessen Wohnung betreten. Das Einverständnis darf nicht durch ein über die Nutzung der Legende hinausgehendes Vortäuschen eines Zutrittsrechts herbeigeführt werden. Im Übrigen richten sich die Befugnisse eines Verdeckten Ermittlers nach diesem Gesetz oder anderen Rechtsvorschriften.
(4) § 9 Absätze 2 und 3 gilt entsprechend. Eine Unterrichtung kann auch unterbleiben, wenn dadurch der weitere Einsatz des Verdeckten Ermittlers oder Leib oder Leben einer Person gefährdet wird.

1

Der Einsatz verdeckter Ermittler ist eine besondere Form der Datenerhebung. Eine Legende im Sinne des Absatzes 1 liegt vor, wenn der Verdeckte Ermittler gezielt, planmäßig und langfristig angelegt über seine Identität oder seinen Auftrag täuscht, um hierdurch das Vertrauen der Personen, gegen die die Maßnahme gerichtet ist, zu erwerben. Das bloße Verschweigen der Zugehörigkeit zur Polizei oder eine nur kurzfristige Täuschung anläßlich einer gezielten Befragung fallen somit noch nicht unter diese Begriffsbestimmung. Es versteht sich von selbst, daß Verdeckte Ermittier ebenso wie Vertrauenspersonen bei der Erfüllung ihres Auftrags keine Straftaten begehen dürfen. Die Voraussetzungen für den Einsatz Verdeckter Ermittler entsprechen denen der §§ 9 bis 11. Allerdings wird die Datenerhebung entsprechend den Besonderheiten beim Einsatz Verdeckter Ermittler nicht von vornherein auf eine bestimmte Person beschränkt. Voraussetzung ist weiter, daß der Einsatz Verdeckter Ermittler entweder zur Abwehr einer unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist oder Tatsachen die Annahme rechtfertigen, daß Straftaten von erheblicher Bedeutung im Sinne des § 1 Absatz 4 begangen werden sollen und der Einsatz zur vorbeugenden Bekämpfung dieser Straftaten erforderlich ist. Die Beschränkung auf den Bereich der organisierten Kriminalität hat sich als zu eng erwiesen. In bestimmten Fällen gibt es zwar Hinweise auf kriminelle Strukturen, die Erkenntnisse reichen aber oft nicht aus, um eine Organisierte Kriminalität belegen zu können. Dies trifft unter anderem auf Täter aus der rechtsextremistischen Szene zu. Häufig verfügen diese Gruppen über einen gewissen Grad an Organisation, jedoch werden von ihnen die Straftaten von erheblicher Bedeutung nicht unbedingt in der Form Organisierter Kriminalität begangen. Dennoch ist bei diesen Ermittlungen beispielsweise der Einsatz verdeckter Ermittler notwendig, um bestimmte Zusammenhänge und Kontakte aufzudecken.

2

Weitergehenden Einschränkungen unterliegt dagegen der zielgerichtete Einsatz gegen eine bestimmte Person, da diese Form des Einsatzes mit einer größeren Intensität des Grundrechtseingriffs verbunden ist. Voraussetzung ist hier, daß Tatsachen die dringende Annahme rechtfertigen, daß diese Person eine Straftat von erheblicher Bedeutung begehen wird. Die „dringende Annahme“ hat dabei eine ähnliche Bedeutung wie der dringende Tatverdacht im Strafverfahrensrecht.

Erforderlich ist somit eine große oder überwiegende Wahrscheinlichkeit. Eine an Sicherheit grenzende Wahrscheinlichkeit wird dagegen nicht vorausgesetzt. Darüber hinaus ist erforderlich, daß eine Aufklärung des Sachverhalts auf andere Weise - also auch unter Einsatz der in den §§ 9 bis 11 geregelten Befugnisse - aussichtlos wäre.

3

Über die in § 9 Absatz 2 festgelegten Verfahrensregelungen hinaus, die nach Absatz 4 entsprechend anzuwenden sind, bedarf der Einsatz im Bereich der vorbeugenden Bekämpfung von Straftaten der Zustimmung der Staatsanwaltschaft. Diese Regelung erfolgt, weil der Einsatz Verdeckter Ermittler eine besonders tiefgreifende Maßnahme darstellt und weil dabei eine etwaige Verwertung in einem künftigen Strafverfahren berücksichtigt werden muß.

4

Absatz 2 erlaubt es, die zum Aufbau oder zur Sicherung der Legende des Verdeckten Ermittlers notwendigen Urkunden (z.B. Personalausweis, Führerschein) herzustellen. Durch die in dieser Bestimmung eingeräumte Befugnis, unter der Legende am Rechtsverkehr teilzunehmen, ensteht Dritten kein zivilrechtlicher Nachteil. Absatz 3 erweitert die Befugnisse des Verdeckten Ermittlers zum Betreten von Wohnungen. Würde ihm nur ein Betretungsrecht nach § 16 HmbSOG zustehen, könnte er beispielsweise der Einladung seiner Zielperson, gemeinsam deren Wohnung aufzusuchen, nicht folgen. Absatz 3 Satz 2 stellt klar, daß der Verdeckte Ermittler den Zutritt zur Wohnung nicht durch Vortäuschen eines sich aus einem anderen Grunde ergebenden Zutrittsrechts herbeiführen darf.

§ 13 Polizeiliche Beobachtung

(1) Die Polizei darf personenbezogene Daten, insbesondere die Personalien einer Person sowie das amtliche Kennzeichen des von ihr benutzten oder eingesetzten Kraftfahrzeuges, zur polizeilichen Beobachtung in einer Datei speichern (Ausschreibung zur polizeilichen Beobachtung), wenn

1. **die Gesamtwürdigung der Person und der von ihr bisher begangenen Straftaten erwarten lassen, dass sie auch künftig Straftaten von erheblicher Bedeutung begehen wird,**
2. **Tatsachen die Annahme rechtfertigen, dass die Person Straftaten von erheblicher Bedeutung begehen wird,**

und dies zur vorbeugenden Bekämpfung dieser Straftaten erforderlich ist.

(2) Im Falle eines Antreffens der Person oder des Kraftfahrzeugs dürfen die Personalien und die von Begleitern, das Kennzeichen des benutzten Kraftfahrzeugs sowie Erkenntnisse über Zeit, Ort, mitgeführten Sachen, Verhalten, Vorhaben und sonstige Umstände des Antreffens an die ausschreibende Polizeibehörde übermittelt werden.

(3) § 9 Absatz 2 gilt entsprechend. Die Anordnung ist auf höchstens ein Jahr zu befristen. Spätestens nach Ablauf von sechs Monaten ist zu prüfen, ob die Voraussetzungen für die Anordnung noch bestehen. Das Ergebnis dieser Prüfung ist aktenkundig zu machen. Zur Verlängerung der Frist bedarf es einer neuen Anordnung.

(4) Liegen die Voraussetzungen für die Anordnung nicht mehr vor, ist der Zweck der Maßnahme erreicht oder zeigt sich, dass er nicht erreicht werden kann, ist die Ausschreibung zur polizeilichen Beobachtung unverzüglich zu löschen. § 9 Absatz 3 gilt entsprechend.

Absatz 1 regelt die Voraussetzungen für die Ausschreibung einer Person zur polizeilichen Beobachtung. Zweck dieser Maßnahme ist es, daß Polizeidienststellen, die die ausgeschriebene Person anläßlich einer nach einer anderen Rechtsvorschrift durchgeführten Kontrolle oder einer anderen Gelegenheit antreffen, diesen Umstand sowie bestimmte weitere Tatsachen mitteilen. Diese Norm erlaubt somit selbst keine Identitätsfeststellung. Besondere datenschutzrechtliche Bedeutung erlangt diese Maßnahme dadurch, daß sie von vorherein auf einen längeren Zeitraum angelegt ist. Wie in § 9 Absatz 2 besteht daher auch hier ein Anordnungsvorbehalt für den Polizeipräsidenten. Die Fortdauer der Ausschreibung bedarf einer Überprüfung in regelmäßigen Abständen. Absatz 4 regelt die Beendigung der Maßnahme sowie eine eventuelle Unterrichtung des Betroffenen.

Dritter Abschnitt

Befugnisse zur weiteren Datenverarbeitung

§ 14 Grundsätze der Zweckbindung

(1) Die Speicherung, Veränderung oder Nutzung darf nur zu dem Zweck erfolgen, zu dem diese Daten erlangt worden sind. Die Nutzung einschließlich einer erneuten Speicherung und einer Veränderung zu einem anderen polizeilichen Zweck ist zulässig, soweit die Polizei die Daten zu diesem Zweck erheben dürfte. Personenbezogene Daten, die in einer Datei gespeichert sind, dürfen für einen anderen als den nach § 26 Absatz 1 Nummer 1 festgelegten Zweck genutzt, erneut gespeichert oder verändert werden, wenn hierdurch erhebliche Nachteile für das Gemeinwohl oder schwer wiegende Beeinträchtigungen von gewichtigen Rechtspositionen einzelner verhindert oder beseitigt werden sollen.

(2) Daten, die mit besonderen Mitteln der Datenerhebung nach den §§ 9 bis 13 sowie nach § 23 erhoben wurden, dürfen für andere Verfahren nur genutzt werden, wenn sie auch dafür unter Einsatz dieser Befugnisse hätten erhoben werden dürfen. Sie dürfen nach Maßgabe bundesgesetzlicher Regelungen auch für gemeinsame Dateien des Bundes und der Länder auf den Gebieten des Staatsschutzes und der organisierten Kriminalität in Fällen von erheblicher Bedeutung einschließlich der Vorfeldbeobachtung genutzt werden; dies gilt auch für Dateien, die nicht in der Verantwortung von Polizeibehörden errichtet werden. Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, sowie Daten, die nach § 5 erhoben wurden, dürfen für andere Zwecke nur genutzt werden, soweit dies zur Abwehr einer unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist oder Anhaltspunkte dafür vorliegen, dass die Verfolgung einer Straftat von erheblicher Bedeutung ansonsten aussichtslos oder wesentlich erschwert wäre.

(3) Werden wertende Angaben in Dateien gespeichert, muss feststellbar sein, bei welcher Stelle die Unterlagen geführt werden, die der Bewertung zugrunde liegen. Das Gleiche gilt, wenn in einer Datei Kurzinformationen über bestimmte Sachverhalte gespeichert werden. Wertende Angaben dürfen nicht allein auf Informationen gestützt werden, die unmittelbar durch automatisierte Datenverarbeitung gewonnen wurden.

1

In § 14 ist der Grundsatz der Zweckbindung bei der Datennutzung festgeschrieben. Danach dürfen Daten grundsätzlich nur für den Zweck genutzt werden, für den sie auch erhoben wurden. Ausnahmen von dieser Regel müssen gesetzlich geregelt sein. Der Begriff „polizeilicher Zweck“ ist dabei im Sinne von § 1 Absatz 3 zu interpretieren. Soweit also Organisationseinheiten innerhalb der Polizei andere als vollzugspolizeiliche Aufgaben erfüllen, ist die Nutzung von Daten für diese Zwecke nicht mehr von dieser Bestimmung umfaßt. Absatz 1 Satz 3 enthält eine Einschränkung gegenüber den in Absatz 1 Satz 2 zugelassenen Zweckänderungen. Daten, die in einer Datei gespeichert sind, dürfen grundsätzlich nur für den in der jeweiligen Errichtungsanordnung festgelegten Zweck genutzt werden. Soll eine Datei mehreren Zwecken dienen (multifunktionelle Zweckbestimmung), so muß dies in der Errichtungsanordnung deutlich hervorgehoben werden. Eine Nutzung für andere Zwecke ist nur unter den im letzten Halbsatz genannten Voraussetzungen zulässig.

2

Absatz 2 enthält besondere Einschränkungen des Gebots der Zweckbindung. Die Einschränkung nach Satz 1 trägt der besonderen Eingriffsqualität dieser Erhebungsmethoden Rechnung. Mit Blick auf die bundesgesetzlich vorgesehene Anti-Terror-Datei soll mit Satz 2 die Übermittlung und Nutzung von Daten aus verdeckten Maßnahmen der allgemeinen Gefahrenabwehr für gemeinsame Dateien des Bundes und der Länder ermöglicht werden. Satz 3 betrifft Daten, die von vornherein nur zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert oder nach § 5 erhoben wurden. Die Nutzung dieser Daten für andere Zwecke ist nur ausnahmsweise zulässig, wenn dies zur Abwehr einer unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person erforderlich oder in einem Ermittlungsverfahren wegen einer Straftat von erheblicher Bedeutung notwendig ist. Letzteres gilt insbesondere für sogenannte Protokolldateien, die zu Zwecken der Datenschutzkontrolle angelegt werden. In solchen Protokolldateien wird jeder Zugriff auf Dateien der Polizei Hamburg gespeichert. Anhand dieser Daten kann anschließend nachvollzogen werden, welche Person und aus welchem Anlass auf die jeweilige Datei zugegriffen hat. Dies ist ein wesentliches Mittel der Datenschutzkontrolle. Jedoch können auch in Strafverfahren solche Daten von Bedeutung sein. So kann anhand von Protokolldateien nachgeprüft werden, wann und warum ein Verdächtiger schon einmal Adressat von polizeilichen Maßnahmen war. Beispielsweise könnte bei einem mutmaßlichen Straftäter, dessen Aufenthaltsort in einem bestimmten Zeitraum ermittelt werden soll, eine Personenkontrolle durchgeführt worden sein. Im Rahmen eines strafrechtlichen Ermittlungsverfahrens kann diese Information von erheblicher Bedeutung sein.

3

Absatz 3 enthält besondere Beschränkungen für die Speicherung wertender Angaben sowie von Kurzinformationen. Hierdurch soll insbesondere der Gefahr einer Verselbständigung dieser Daten von den zugrundeliegenden Sachverhalten vorgebeugt werden.

§ 15 Dauer der Datenspeicherung

Daten dürfen solange gespeichert werden, wie es für die Aufgabenerfüllung erforderlich ist. Für automatisierte Dateien sind Fristen festzulegen, nach deren Ablauf spätestens überprüft werden muss, ob die suchfähige Speicherung von Daten weiterhin erforderlich ist (Prüfungsfristen). Für nicht automatisierte Dateien und Akten sind Prüfungsfristen oder Aufbewahrungsfristen festzulegen. Dabei sind der Speicherungszweck sowie Art und Bedeutung des Anlasses der Speicherung zu berücksichtigen. Prüfungsfristen oder Aufbewahrungsfristen für suchfähig gespeicherte personenbezogene Daten von Kindern dürfen zwei Jahre nicht überschreiten; die Frist beginnt mit dem Tag der ersten Speicherung. Nach Ablauf der Prüfungsfristen ist eine weitere Speicherung nur zulässig, wenn dies wegen besonderer Gründe im Einzelfall erforderlich ist.

In Satz 1 wird als Grundregel vorgegeben, die Speicherungsdauer auf das erforderliche Maß zu beschränken. Eine darüber hinausgehende differenzierte gesetzliche Normierung über die Speicherdauer für alle bei der Polizei vorhandenen automatisierten oder nicht-automatisierten Dateien sowie Akten und Aktensammlungen unter Berücksichtigung von deren jeweiliger Zweckbestimmung wäre zu unflexibel, um den datenschutzrechtlichen Belangen wie den Anforderungen der polizeilichen Praxis im einzelnen angemessen Rechnung tragen zu können. Diese Bestimmung beschränkt sich daher auf die Verpflichtung, Prüfungstermine oder Aufbewahrungsfristen festzulegen, zu denen die Erforderlichkeit der weiteren Speicherung des jeweiligen Datums zu überprüfen ist. Suchfähig gespeicherte Daten sind solche, die unter Verwendung des Namens, eines personenbeziehbaren Aktenzeichens oder eines Hilfsmerkmals jederzeit gezielt aufgefunden werden können. Nicht unter diesen Begriff fallen somit Angaben, die als Beiwerk in einem Sachvorgang oder in einer zu einer anderen Person angelegten Akte enthalten sind und dort nur zufällig - anläßlich eines sonstigen Zugriffs auf diese Akte - aufgefunden werden können. Eine besondere Einschränkung enthält die Bestimmung nur für die suchfähig gespeicherten Daten von Kindern. Hier hat in jedem Fall spätestens nach zwei Jahren eine Überprüfung zu erfolgen. Satz 5 verdeutlicht, daß Daten nach Erreichen des Prüfungstermins regelmäßig gelöscht werden sollen. Eine weitere Speicherung und Nutzung soll nur zulässig sein, wenn dies im Einzelfall aus besonderen Gründen auch über den Prüfungstermin hinaus erforderlich ist.

§ 16 Speichern, Verändern und Nutzen von Daten

(1) Die Polizei darf personenbezogene Daten in Akten oder Dateien speichern, verändern und nutzen, soweit dies zur Erfüllung ihrer Aufgaben, einschließlich einer zeitlich befristeten Dokumentation oder der Vorgangsverwaltung erforderlich ist.

(2) Dabei darf die Polizei auch die im Rahmen der Verfolgung von Straftaten gewonnenen personenbezogenen Daten zum Zwecke der Gefahrenabwehr (§ 1 Absatz 1) speichern, verändern und nutzen. Soweit die Daten ausschließlich auf Grund von Befugnissen erhoben wurden, die den in §§ 9 bis 13 und § 23 genannten Befugnissen entsprechen, dürfen sie für andere Verfahren nur genutzt werden, wenn sie auch dafür unter Einsatz dieser Befugnisse hätten erhoben werden dürfen. Eine suchfähige Speicherung dieser Daten in Dateien und Akten ist nur über Personen zulässig, gegen die ein strafrechtliches Ermittlungsverfahren eingeleitet worden ist und bei denen wegen der Art, Ausführung oder Schwere der Tat und der Persönlichkeit des Betroffenen die Besorgnis der Begehung weiterer Straftaten besteht. Entfällt der dem Ermittlungsverfahren zugrunde liegende Verdacht, sind die Daten zu löschen. Die nach § 15 festzulegenden Prüfungstermine dürfen bei Erwachsenen 10 Jahre und bei Jugendlichen 5 Jahre nicht überschreiten. Die Frist beginnt mit dem Tag, an dem das letzte Ereignis eingetreten ist, das zur Speicherung der Daten geführt hat, jedoch nicht vor Entlassung des Betroffenen aus einer Justizvollzugsanstalt oder Beendigung einer mit Freiheitsentziehung verbundenen Maßregel der Besserung und Sicherung.
(3) Die Polizei darf personenbezogene Daten von Kontakt- oder Begleitpersonen einer Person, bei der tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass sie künftig Straftaten begehen wird, sowie über Auskunftspersonen in Dateien suchfähig speichern, verändern und nutzen, soweit dies zur vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung unerlässlich ist. Die Speicherungsdauer darf drei Jahre nicht überschreiten. Nach jeweils einem Jahr, gerechnet vom Zeitpunkt der letzten Speicherung, ist zu prüfen, ob die Voraussetzungen nach Satz 1 noch vorliegen; die Entscheidung kann nur durch einen besonders ermächtigten Bediensteten getroffen werden.

1

In Absatz 1 wird die allgemeine Befugnis für die Polizei geschaffen, personenbezogene Daten in Akten oder Dateien zu speichern, soweit dies für ihre Aufgabenerfüllung erforderlich ist. Gemeint sind hiermit die der Polizei nach § 1 obliegenden Aufgaben. Die Speicherung von Daten zur Vorgangsverwaltung und zur Dokumentation ist ein untrennbarer Bestandteil der polizeilichen Aufgabenerfüllung. Aus Gründen der Klarstellung werden diese Zwecke allerdings an dieser Stelle besonders hervorgehoben. Soweit Daten ausschließlich zu diesen Zwecken gespeichert werden, unterliegen sie auch der entsprechenden Zweckbindung. Sie dürfen somit nur unter den Voraussetzungen des § 14 Absatz 1 Satz 2 für andere Zwecke genutzt werden.

2

Absatz 2 erlaubt die Verarbeitung von Daten, die die Polizei im Rahmen der Verfolgung von Straftaten erlangt hat, zu Zwecken der Gefahrenabwehr. Der Klammerhinweis auf § 1 Absatz 1 verdeutlicht, daß zur Gefahrenabwehr auch die vorbeugende Bekämpfung von Straftaten, also die Verhütung von Straftaten und die Vorsorge für die Verfolgung künftiger Straftaten gehört. Hauptanwendungsfall dieser Bestimmung ist das Anlegen von Kriminalakten sowie Einrichtung und Betrieb einer Datei über vorhandene Kriminalakten. Hierin dürfen nur Personen, gegen die ein

straftrechtliches Ermittlungsverfahren eingeleitet worden ist, also Täter oder Tatverdächtige, erfaßt werden. Die suchfähige Speicherung von in Ermittlungsverfahren erlangten Daten weiterer Personen ist nur unter den Vorausetzungen des Absatzes 3 zulässig. In Absatz 2 Sätze 3 und 4 werden für diesen Bereich Höchstfristen für Prüfungstermine gesetzlich vorgegeben. Satz 2 enthält eine Konkretisierung der sich bereits aus § 14 Absatz 2 Satz 1 ergebenden besonderen Zweckbindung. Der Anwendungsbereich ist allerdings auf solche Daten beschränkt, die ausschließlich unter Anwendung solcher Erhebungsbefugnisse erlangt wurden. Die suchfähige Speicherung von Dateien über Kontakt- und Begleitpersonen sowie Auskunftspersonen ist nur unter den weiteren Einschränkungen des Absatzes 3 zulässig. Hiervon unberührt ist allerdings eine Speicherung von Daten dieser Personen (z.B. als Geschädigte oder Zeugen) zum Zwecke der Vorgangsverwaltung oder in nicht suchfähiger Form, deren Zulässigkeit sich nach Absatz 1 bestimmt.

§ 17 Nutzung von Daten zu Zwecken der Statistik, Aus- und Fortbildung
(1) Die Polizei darf personenbezogene Daten auch über die nach anderen Vorschriften zulässige Speicherungsdauer hinaus zur Aus- und Fortbildung nutzen. Dabei ist sicherzustellen, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr einer bestimmten oder bestimmbaren Person zugeordnet werden können (Anonymisierung). Die Anonymisierung kann unterbleiben, wenn diese nicht mit vertretbarem Aufwand möglich ist oder dem Aus- und Fortbildungszweck entgegensteht und jeweils die schutzwürdigen Belange des Betroffenen nicht offensichtlich überwiegen.
(2) Die Polizei darf gespeicherte personenbezogene Daten zu statistischen Zwecken nutzen; die Daten sind zum frühestmöglichen Zeitpunkt zu anonymisieren. Eine Veröffentlichung ist nur zulässig, wenn kein Rückschluss auf die Verhältnisse einer natürlichen Person möglich ist.

Aus verfassungsrechtlichen Gründen bedarf auch die Nutzung personenbezogener Daten zu diesen Zwecken einer gesetzlichen Grundlage. Die Beschränkung der Anonymisierungspflicht nach Absatz 1 trägt dem Umstand Rechnung, daß in bestimmten Bereichen der Aus- und Fortbildung mit fiktiven oder vollständig anonymisierten Daten (z.B. geschwärzte bzw. gelöschte Daten auf Schriftstücken oder unkenntlich gemachte Gesichter auf Filmaufnahmen) nicht möglich ist. Insoweit müssen hier auch in beschränktem Umfang Originalunterlagen genutzt werden können. Demgegenüber ist bei einer Nutzung von Daten zu statistischen Zwecken der Personenbezug möglichst frühzeitig durch Anonymisierung aufzuheben.

§ 18 Allgemeine Regelungen der Datenübermittlung
(1) Die Polizei darf personenbezogene Daten, soweit gesetzlich nichts anderes bestimmt ist, nur zu dem Zweck übermitteln, zu dem sie die Daten erlangt oder gespeichert hat. § 14 Absatz 2 gilt entsprechend. Datenübermittlung im Sinne dieses Gesetzes ist auch die Weitergabe polizeilicher Daten innerhalb der zuständigen Behörde an andere als die in § 1 Absatz 3 genannten Organisationseinheiten.
(2) Bewertungen sowie die nach § 16 Absatz 3 gespeicherten personenbezogenen Daten dürfen nur an Polizeidienststellen und andere mit Aufgaben der Strafverfolgung beauftragte Stellen übermittelt werden.

(3) Unterliegen die personenbezogenen Daten einem Berufs- oder besonderem Amtsgeheimnis und sind sie der Polizei von der zur Verschwiegenheit verpflichteten Person in Ausübung ihrer Berufs- oder Amtspflicht übermittelt worden, ist die Datenübermittlung durch die Polizei nur zulässig, wenn der Empfänger die Daten zur Erfüllung des gleichen Zwecks benötigt, zu dem sie die Polizei erlangt hat.
(4) Die Verantwortung für die Übermittlung trägt die Polizei. Diese prüft die Zulässigkeit der Datenübermittlung. Erfolgt die Datenübermittlung auf Grund eines Ersuchens des Empfängers, hat dieser die zur Prüfung erforderlichen Angaben zu machen. Bei Ersuchen von Polizeidienststellen sowie anderen Behörden und öffentlichen Stellen prüft die Polizei nur, ob das Ersuchen im Rahmen der Aufgaben des Empfängers liegt, es sei denn, im Einzelfall besteht Anlass zu einer weitergehenden Überprüfung. Erfolgt die Datenübermittlung durch automatisierten Abruf, trägt der Empfänger die Verantwortung für die Rechtmäßigkeit des Abrufs.
(5) Der Empfänger darf die übermittelten personenbezogenen Daten, soweit gesetzlich nichts anderes bestimmt ist, nur zu dem Zweck nutzen, zu dem sie ihm übermittelt worden sind. Ausländische öffentliche Stellen, über- und zwischenstaatliche Stellen sowie Personen und Stellen außerhalb des öffentlichen Bereichs sind bei der Datenübermittlung darauf hinzuweisen.

1

Die Vorschrift regelt die allgemeinen Grundsätze der Datenübermittlung, die bei der Anwendung der folgenden §§ 19 bis 21 zusätzlich zu den dort genannten Voraussetzungen jeweils zu beachten sind. In Absatz 1 werden der Gesetzesvorbehalt sowie der Grundsatz der Zweckbindung hervorgehoben. Datenübermittlungen zu einem anderen Zweck als dem, zu dem die Polizei die Daten erhoben und weiter verarbeitet hat, sind nur unter den in diesem Gesetz geregelten Voraussetzungen zulässig. Die Gleichsetzung von Datenübermittlungen mit der Nutzung von Daten für andere als polizeiliche Zwecke in Satz 3 ist eine Konsequenz aus den Begriffsbestimmungen des Hamburgisehen Datenschutzgesetzes. Da sich der Begriff „Stelle“ am verwaltungs-verfahrensrechtlichen Behördenbegriff orientiert, ist die Weitergabe von Daten innerhalb der zuständigen Behörde keine Datenübermittlung im Sinne des Datenschutzrechts, sondern eine Nutzung. Im Interesse einer praktikablen Abgrenzung - auch im Hinblick auf das Gebot der Zweckbindung - ist es daher sachgerecht, die Weitergabe polizeilicher Daten innerhalb der zuständigen Behörde an nicht-polizeiliche Dienststellen einer Datenübermittlung gleichzustellen.

2

Absatz 2 enthält Einschränkungen des Adressatenkreises für Bewertungen sowie die nach § 16 Absatz 3 gespeicherten Daten. „Andere mit Aufgaben der Strafverfolgung beauftragte Stellen“ sind andere Stellen außerhalb der Hamburger Polizei, deren Mitarbeiter zu Hilfsbeamten der Staatsanwaltschaft (§ 152 GVG) bestellt sind (z.B. die Zollfahndung), aber auch die Staatsanwaltschaft selbst. Absatz 3 berücksichtigt die Zweckbindung von Daten, die einem Berufs- oder besonderen Amtsgeheimnis (z.B. Personalakten-, Sozial- oder Steuergeheimnis) unterliegen. Nicht unter diese Bestimmung fällt die allgemeine beamten- oder verwaltungs-verfahrensrechtliche Geheimhaltungspflicht. Die in Absatz 4 enthaltene Verantwortungsteilung zwischen

dem Empfänger und der übermittelnden Stelle entspricht den Regelungen in anderen vergleichbaren Bestimmungen (z.B. § 14 Absatz 3 des Hamburgischen Datenschutzgesetzes). Die Regelung in Absatz 5 soll die Zweckbindung übermittelter Daten auch nach einer Übermittlung sicherstellen. Keiner besonderen Regelung in diesem Gesetz bedarf die Übermittlung personenbezogener Daten durch andere Behörden oder öffentliche Stellen an die Polizei. Dies ist in den für die übermittelnden Behörden maßgeblichen Rechtsvorschriften geregelt.

§ 19 Datenübermittlung zwischen Polizeidienststellen
(1) An andere Polizeidienststellen dürfen personenbezogene Daten übermittelt werden, soweit dies zur Erfüllung polizeilicher Aufgaben erforderlich ist.
(2) Der Senat wird ermächtigt, durch Rechtsverordnung zu bestimmen, dass Datenübermittlungen an Polizeibehörden bestimmter ausländischer Staaten unter den Voraussetzungen des Absatzes 1 zulässig sind, wenn dies wegen der internationalen polizeilichen Zusammenarbeit erforderlich ist und kein Grund zu der Annahme besteht, dass die Daten von den ausländischen Polizeibehörden entgegen dem Zweck eines deutschen Gesetzes im Geltungsbereich des Grundgesetzes verwandt werden.

Diese Bestimmung betrifft nur die Datenübermittlung an außerhamburgische Polizeidienststellen, da die Hamburger Polizei als eine Stelle gilt und somit die Weitergabe von Daten innerhalb der Hamburger Polizei als Nutzung, nicht als Datenübermittlung im Sinne dieses Gesetzes zu bewerten ist. Die Bestimmung enthält - anders als die nachfolgenden Regelungen - im Hinblick auf die Aufgabenparallelität keine besonderen Voraussetzungen für die Zulässigkeit einer Datenübermittlung. Die Verordnungsermächtigung nach Absatz 2 soll eine differenzierte Behandlung von Datenübermittlungen an Polizeibehörden ausländischer Staaten ermöglichen. Hierdurch soll zugleich die für die Übermittlung zuständige Organisationseinheit der Polizei von der Verantwortung für die Prüfung der Frage entlastet werden, ob in bestimmten anderen ausländischen Staaten vergleichbare Datenschutzregelungen bestehen oder die Gefahr einer rechtsstaatswidrigen Verfolgung besteht.

§ 20 Datenübermittlung an öffentliche Stellen, an ausländische öffentliche Stellen sowie an über- und zwischenstaatliche Stellen
(1) Die Polizei darf personenbezogene Daten an öffentliche Stellen übermitteln, soweit dies erforderlich ist
1. zur Erfüllung polizeilicher Aufgaben,
2. zur Abwehr einer bevorstehenden Gefahr durch den Empfänger,
3. zur Teilnahme am Privatrechtsverkehr oder zur Durchsetzung öffentlich-rechtlicher Geldforderungen und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an der Geheimhaltung überwiegt,
4. in besonders gelagerten Einzelfällen zur Feststellung der gesetzlichen Voraussetzungen für den Erlass eines Verwaltungsaktes durch eine andere für Aufgaben der Gefahrenabwehr zuständige öffentliche Stelle, oder
5. zur Verhütung oder Beseitigung erheblicher Nachteile für das Gemeinwohl oder schwer wiegender Beeinträchtigungen von gewichtigen Rechtspositionen einzelner, insbesondere zur Abwehr von Gefahren für

Leib, Leben, Gesundheit, persönliche Freiheit oder erhebliche Vermögenswerte.

Die Übermittlung zu einem anderen Zweck, als dem, zu dem die Polizei die Daten erlangt oder gespeichert hat, ist nur zulässig, wenn der Empfänger die Daten auf andere Weise

1. **nicht oder nicht rechtzeitig erlangen kann oder**
2. **nur mit unverhältnismäßig hohem Aufwand erlangen kann und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen des Betroffenen beeinträchtigt würden.**

In den Fällen von Satz 1 Nummern 1 und 4 ist die Übermittlung zu einem anderen Zweck darüber hinaus nur zulässig, wenn die Übermittlung zur Abwehr einer bevorstehenden Gefahr erforderlich ist.

(2) Die Polizei darf personenbezogene Daten, die sie anlässlich ihrer Aufgabenerfüllung erlangt hat, an andere für Aufgaben der Gefahrenabwehr zuständige öffentliche Stellen übermitteln, soweit die Kenntnis dieser Daten zur Erfüllung der Aufgaben des Empfängers erforderlich erscheint.

(3) Die Polizei darf personenbezogene Daten an ausländische öffentliche Stellen sowie an über- und zwischenstaatliche Stellen übermitteln, soweit

1. **dies zur Erfüllung polizeilicher Aufgaben erforderlich ist,**
2. **sie hierzu auf Grund über- oder zwischenstaatlicher Vereinbarungen über Datenübermittlungen zwischen Polizeidienststellen berechtigt oder verpflichtet ist, oder**
3. **dies zur Abwehr einer erheblichen Gefahr durch den Empfänger erforderlich ist.**

Absatz 1 Sätze 2 und 3 gilt entsprechend. Die Datenübermittlung unterbleibt, soweit Grund zu der Annahme besteht, dass dadurch gegen den Zweck eines deutschen Gesetzes verstoßen würde oder schutzwürdige Interessen des Betroffenen beeinträchtigt würden.

(4) Anderweitige besondere Rechtsvorschriften über die Datenübermittlung an öffentliche Stellen bleiben unberührt.

1

Diese Bestimmung erfaßt nur Datenübermittlungen der Polizei an andere Behörden und öffentliche Stellen, für die es keine spezialgesetzlichen Regelungen gibt. Absatz 1 erlaubt unter den dort genannten Voraussetzungen eine Datenüberrnittlung an andere Behörden oder öffentliche Stellen. Die Vorschrift unterscheidet dabei nicht zwischen Übermittlungen von Amts wegen, also aus eigener Initiative der Polizei, und Übermittlungen auf Ersuchen. Entscheidend für die Zulässigkeit ist allein, ob die jeweiligen tatbestandlichen Voraussetzungen erfüllt sind. Auf wessen Veranlassung die Übermittlung erfolgt, ist demgegenüber nachrangig. Allerdings wird den Übermittlungen nach Absatz 1 Nummern 2 bis 5 in aller Regel ein Ersuchen des Empfängers vorangehen, da die Polizei in diesen Fällen ohne entsprechende Angaben des Empfängers nicht in der Lage sein wird, die Zulässigkeit einer Übermittlung zu beurteilen (vgl. § 18 Absatz 4).

2

Nach Absatz 1 Nummer 1 ist die Datenübermittlung zur Erfüllung polizeilicher Aufgaben zulässig. Dies betrifft insbesondere Fälle, in denen die Erfüllung einer bestimmten polizeilichen Aufgabe die Unterrichtung einer anderen Stelle erfordert.

Absatz 1 Nummer 2 setzt voraus, daß der Empfänger die Angaben zur Abwehr einer konkreten Gefahr benötigt. Absatz Nummer 3 soll sicherstellen, daß die öffentliche Hand als Teilnehmer am Privatrechtsverkehr bzw. Behörden als Gläubiger öffentlich-rechtlicher Forderungen nicht schlechter gestellt werden als Privatpersonen, denen unter den Voraussetzungen von § 21 personenbezogene Daten übermittelt werden können. Für die Übermittlung nach Absatz 1 Nummer 4 ist anders als bei Übermittlungen nach Absatz 1 Nummer 2 eine konkrete Gefahr nicht erforderlich, allerdings wird die Übermittlung auf besonders gelagerte Einzelfälle beschränkt. Insbesondere betrifft dies Datenübermittlungen an Genehmigungs- oder Überwachungsbehörden, wenn diese auf Auskünfte der Polizei angewiesen sind, um z.B. die Zuverlässigkeit einer Person o.ä. persönliche Eigenschaften (vgl. z.B. nach § 35 GewO, § 4 GastG) beurteilen zu können, wenn dies für eine sachgerechte Entscheidung erforderlich ist. Absatz 1 Nummer 5 entspricht der Regelung in § 13 Absatz 2 Satz 1 Nummer 4 des Hamburgischen Datenschutzgesetzes. Sie setzt noch keine konkrete Gefahr voraus, dafür aber eine Gefährdung gewichtiger Interessen.

3

Die Übermittlung zu einem anderen Zweck ist nur unter den Voraussetzungen von Absatz 1 Sätze 2 und 3 zulässig. Die Datenübermittlung nach Absatz 2 betrifft insbesondere die Fälle, in denen die Polizei im Rahmen ihrer Aufgabenerfüllung - sowohl anläßlich einer Datenerhebung bei Maßnahmen des ersten Zugriffs als auch anläßlich einer sonstigen polizeilichen Maßnahme - Kenntnis von einem Sachverhalt erlangt hat, der das Einschreiten der originär zuständigen Behörde erfordert. Da die Polizei nicht von sich aus beurteilen kann, ob im Einzelfall ein Einschreiten der anderen Gefahrenabwehrbehörde wirklich erforderlich ist, setzt diese Bestimmung nur voraus, daß diese aus der Sicht der Polizei erforderlich erscheint. Bei der Datenübermittlung nach dieser Vorschrift wird in der Regel von einer Zweckidentität ausgegangen werden können, da die Kenntniserlangung von einem Sachverhalt sich auf die gleiche Gefahrenlage bezieht wie das spätere Handeln der sachlich zuständigen Gefahrenabwehrbehörde (z.B. die Polizei bemerkt anläßlich eines Einsatzes wegen ruhestörenden Lärms ein verwahrlostes Kind und unterrichtet das zuständige Jugendamt, damit dieses die erforderlichen Maßnahmen der Jugendhilfe einleiten kann).

4

In Absatz 3 werden die Voraussetzungen für Übermittlungen an ausländische öffentliche Stellen sowie an über- und zwischenstaatliche Stellen gegenüber Absatz 1 enger eingegrenzt. Sie sind unzulässig, wenn gegen den Zweck eines deutschen Gesetzes verstoßen würde oder die schutzwürdigen Belange des Betroffenen beeinträchtigt würden (z.B. Gefahr einer rechtsstaatswidrigen Verfolgung durch Behörden des Empfängerlandes). Absatz 4 enthält eine notwendige Klarstellung.

§ 21 Datenübermittlung an Stellen außerhalb des öffentlichen Bereichs
Die Polizei darf personenbezogene Daten an Stellen außerhalb des öffentlichen Bereichs übermitteln, soweit

1. **dies zur Erfüllung polizeilicher Aufgaben erforderlich ist,**
2. **dies zur Verhütung oder Beseitigung erheblicher Nachteile für das Gemeinwohl oder schwer wiegender Beeinträchtigungen von gewichtigen Rechtspositionen einzelner, insbesondere zur Abwehr von Gefahren für Leib, Leben, Gesundheit, persönliche Freiheit oder erhebliche Vermögenswerte, erforderlich ist,**
3. **der Auskunftsbegehrende ein rechtliches Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und die schutzwürdigen Interessen des Betroffenen nicht überwiegen,**
4. **der Auskunftsbegehrende ein berechtigtes Interesse geltend macht und offensichtlich ist, dass die Datenübermittlung im Interesse des Betroffenen liegt und er in Kenntnis der Sachlage seine Einwilligung hierzu erteilen würde.**

§ 20 Absatz 1 Sätze 2 und 3 gilt entsprechend.

Diese Bestimmung behandelt insbesondere die Datenübermittlung an private Empfänger (natürliche Personen) sowie an juristische Personen des Privatrechts. Die Nummern 1 und 2 betreffen insbesondere Datenübermittlungen, die die Polizei aus eigener Initiative vornimmt. Die Nummern 3 und 4 betreffen Fälle, in denen eine Person oder Stelle an die Polizei herantritt und um Auskünfte zu einem bestimmten Sachverhalt bittet, der eine andere Person betrifft. Die schutzwürdigen Belange des Betroffenen sind hierbei nach einem objektiven Durchschnittsmaßstab zu bestimmen. Besondere Empfindlichkeit oder Desinteresse des Betroffenen haben somit außer Betrachtung zu bleiben. Die schutzwürdigen Belange können insbesondere dann überwiegen, wenn sich der Betroffene im Falle einer Datenübermittlung in seinen schutzwürdigen Interessen beeinträchtigt fühlt. Demgegenüber werden bei der Weitergabe von Daten, die zur Durchführung zivilrechtlicher Ansprüche benötigt werden (z.B. personenbezogene Daten, die die Polizei zum Schutzprivater Rechte erhoben hat), die Interessen des Betroffenen in der Regel zurückstehen müssen.

§ 22 Datenabgleich
(1) Die Polizei darf personenbezogene Daten der für eine Gefahr Verantwortlichen sowie der in § 6 Nummer 6 genannten Personen mit dem Inhalt polizeilicher Dateien abgleichen. Personenbezogene Daten anderer Personen darf die Polizei nur abgleichen, wenn Tatsachen die Annahme rechtfertigen, dass dies zur Erfüllung einer bestimmten polizeilichen Aufgabe erforderlich ist. Die Polizei darf rechtmäßig erlangte personenbezogene Daten mit dem Fahndungsbestand abgleichen.
(2) Wird der Betroffene zur Durchführung einer nach einer anderen Rechtsvorschrift zulässigen Maßnahme angehalten und kann der Datenabgleich mit dem Fahndungsbestand nicht bis zum Abschluss dieser Maßnahme vorgenommen werden, darf der Betroffene weiterhin für den Zeitraum festgehalten werden, der regelmäßig für die Durchführung eines Datenabgleiches notwendig ist.
(3) Rechtsvorschriften über den Datenabgleich in anderen Fällen bleiben unberührt.

1

Datenabgleich im Sinne dieser Vorschrift ist die Prüfung, ob zu einer bestimmten Person personenbezogene Daten in einer polizeilichen Datei gespeichert sind. Absatz 1 enthält die Rechtsgrundlage für diese besondere Form der Datenverarbeitung. Diese Bestimmung regelt weder die Erhebung der abzugleichenden Daten noch deren weitere Verarbeitung. Die Polizei kann demnach nur Daten abgleichen, die sie zuvor zulässigerweise erlangt hat. Die Speicherung dieser Daten ist nur unter den Voraussetzungen des § 16 zulässig. Der Datenabgleich nach dieser Bestimmung bewirkt somit nur einen geringen selbständigen Eingriff in das Recht auf informationelle Selbstbestimmung. Nach Absatz 1 Satz 1 können die Daten der dort genannten Personengruppen (Störer und potentielle Straftäter) mit dem Inhalt polizeilicher Dateien abgeglichen werden. Die Daten anderer Personen dürfen nach Satz 2 nur unter eingeschränkten Voraussetzungen abgeglichen werden. Demgegenüber enthält Satz 3 eine Erweiterung. Der Abgleich mit dem Fahndungsbestand, also mit den Dateien, in denen die Daten von Personen, nach denen die Polizei fahndet, sowie gesuchter Gegenstände gespeichert sind, ist bei allen Personen zulässig, von denen die Polizei zulässigerweise Daten erlangt hat.

2

Das Anhalterecht nach Absatz 2 ergänzt das Anhalterecht nach anderen Bestimmungen (z.B. § 4 Absatz 3 Satz 2 Nummer 1). Es gilt nur für die Zeit, die üblicherweise für einen Abgleich benötigt wird. Eine darüber hinausgehende Freiheitsbeschränkung ist nach dieser Vorschrift nicht zulässig. Absatz 3 enthält eine notwendige Klarstellung. Von dieser Bestimmung wird auch erfaßt der in § 15 der Verordnung über regelmäßige Datenübermittlungen aus dem Melderegister geregelte Datenabgleich von bestimmten Meldedaten mit dem Inhalt polizeilicher Daten. Die Forderung nach bereichsspezifischen Regelungen setzt nicht notwendig voraus, daß die Regelung im Polizeirecht erfolgt. Da dieser Abgleich sowohl eine melderechtliche als auch eine polizeirechtliche Komponente hat, kann diese Regelung auch im Melderecht getroffen werden. Auch aus regelungssystematischen Gründen ist die jetzige Regelung im Melderecht vorzuziehen, da in der genannten Verordnung alle auf Landesrecht beruhenden regelmäßigen Datenübermittlungen aus dem Melderegister zusammengefaßt sind.

§ 23 Rasterfahndung

(1) Die Polizei darf von öffentlichen und nichtöffentlichen Stellen zur Verhütung von Straftaten erheblicher Bedeutung,

1. die sich gegen den Bestand oder die Sicherheit des Bundes oder eines Landes richten oder

2. bei denen Schäden für Leib, Leben oder Freiheit zu erwarten sind,

die Übermittlung von personenbezogenen Daten bestimmter Personengruppen zum Zwecke des automatisierten Abgleichs mit anderen Datenbeständen verlangen (Rasterfahndung), wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass dies zur Verhütung dieser Straftaten erforderlich ist.

(2) Die Merkmale, die für den Abgleich oder die Auswertung maßgeblich sein sollen, sind zuvor schriftlich festzulegen. Das Übermittlungsersuchen ist auf Namen, Vornamen, Geburtsdatum, Geburtsort und Anschrift sowie auf im

Einzelfall festzulegende Merkmale zu beschränken; es darf sich nicht auf personenbezogene Daten erstrecken, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen. Vom Übermittlungsersuchen nicht erfasste personenbezogene Daten dürfen übermittelt werden, wenn wegen erheblicher technischer Schwierigkeiten oder wegen eines unangemessenen Zeit- oder Kostenaufwandes eine Beschränkung auf die angeforderten Daten nicht möglich ist; diese Daten dürfen von der Polizei nicht weiterverarbeitet werden. § 10 SOG gilt entsprechend.
(3) Ist der Zweck der Maßnahme erreicht oder zeigt sich, dass er nicht erreicht werden kann, sind die übermittelten und im Zusammenhang mit der Maßnahme zusätzlich angefallenen Daten zu löschen und die Akten zu vernichten, soweit sie nicht für ein mit dem Sachverhalt zusammenhängendes Verfahren erforderlich sind. Hierüber ist eine Niederschrift anzufertigen. Diese Niederschrift ist gesondert aufzubewahren.
(4) Die Maßnahme darf nur von dem Präses oder dem Staatsrat der für die Polizei zuständigen Fachbehörde angeordnet werden. Nach Abschluss der Maßnahme wird der Hamburgische Datenschutzbeauftragte unverzüglich unterrichtet.
(5) Nach Durchführung des Abgleichs sind die von weiterführenden polizeilichen Maßnahmen betroffenen Personen hiervon zu unterrichten, soweit dadurch nicht die Erfüllung polizeilicher Aufgaben vereitelt oder erheblich gefährdet würde oder sich an den auslösenden Sachverhalt ein strafrechtliches Ermittlungsverfahren anschließt.

1

§ 23 regelt die Rasterfahndung zur polizeilichen Gefahrenabwehr. Obwohl hierdurch zunächst eine Vielzahl von Unbeteiligten betroffen ist, sind die Voraussetzungen nach Absatz 1 relativ weit gefaßt. Die Maßnahme muß zur Verhütung von Straftaten erheblicher Bedeutung erforderlich sein. Eine unmittelbar bevorstehende Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person ist nicht mehr Voraussetzung. Der Begriff der „unmittelbar bevorstehenden Gefahr“ ist inhaltlich weitgehend identisch mit dem Begriff der „gegenwärtigen Gefahr“. Die Rechtsprechung bezeichnet eine Gefahr als gegenwärtig, wenn die Einwirkung des schädigenden Ereignisses unter anderem unmittelbar oder in allernächster Zeit mit einer an Sicherheit grenzenden Wahrscheinlichkeit bevorsteht (vgl. VG Hamburg in seiner Entscheidung zur Rechtmäßigkeit der Rasterfahndung vom 27. Februar 2002 - Az. 14 VG 446/2002 -). Nach den Anschlägen von New York am 11. September 2001 wurde vom Präses der Innenbehörde am 19. September 2001 und 15. Oktober 2001 die Rasterfahndung angeordnet. Die Zulässigkeit der Rasterfahndung wurde vom VG Hamburg in der Entscheidung vom 27. Februar 2002 bestätigt. Nach Auffassung des Gerichts lag zum Zeitpunkt der Anordnung eine „unmittelbar bevorstehende Gefahr“ vor. Das Gericht begründete dies damit, daß in einem so kurzen Zeitraum nach den Anschlägen vom 11. September 2001 die Gefahr für weitere Gewaltakte nicht abgeklungen sei. In Hessen hatte demgegenüber das Landgericht Wiesbaden mit Beschluss vom 6. Februar 2002 eine derartige Anordnung mit der Begründung aufgehoben, es liege keine gegenwärtige Gefahr vor. Das Oberlandesgericht Frankfurt am Main hatte diese Entscheidung mit Beschluss vom 21. Februar 2002 bestätigt, sodaß in Hessen die Rasterfahndung abgebrochen werden mußte. Diese uneinheitliche Rechtsprechung zum Vorliegen der Voraussetzungen der Rasterfahndung und die Erkenntnis, daß die Rasterfahn-

dung ein notwendiges und effektives Instrument der Gefahrenabwehr gegen den internationalen Terrorismus bietet, machten eine Herabsetzung der Eingriffsvoraussetzungen notwendig. Nur so kann gewährleistet werden, daß auch in Zukunft auf die aktuelle weltpolitische Sicherheitslage reagiert werden kann. Die Rasterfahndung nach § 23 hat sich bei der Terroristenfahndung bewährt. Mit dieser polizeilichen Maßnahme konnten wichtige Erkenntnisse über die Strukturen des internationalen Terrorismus und die Verbindungen nach Hamburg gewonnen werden. Es widerspricht der Aufgabe und Effektivität polizeilicher Gefahrenabwehr, wenn eine Rasterfahndung zukünftig nur zulässig sein sollte, nachdem es schon zu Anschlägen gekommen ist. Ziel der Rasterfahndung nach § 23 ist es gerade, solche Anschläge zu verhindern. Die Rasterfahndung darf daher nicht an das Vorliegen einer „unmittelbar bevorstehenden“ oder „gegenwärtigen“ Gefahr gekoppelt sein. Ein präventives Vorgehen gegen den internationalen Terrorismus muß auch zulässig sein, wenn das schädigende Ereignis nicht unmittelbar oder in allernächster Zeit mit einer an Sicherheit grenzenden Wahrscheinlichkeit bevorsteht. Das Bundesverfassungsgericht hat der Rasterfahndung allerdings Grenzen gesetzt. Dieser präventive polizeiliche Datenvergleich sei nur dann mit dem Grundrecht auf informationelle Selbstbestimmung vereinbar, wenn eine konkrete Gefahr für Rechtsgüter wie den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leben, Leib oder Freiheit einer Person vorliege. Eine allgemeine Bedrohungslage, wie sie nach den Anschlägen vom 11. September 2001 durchgehend bestanden habe, oder außenpolitische Spannungen reichten für die Anordnung einer Rasterfahndung nicht aus (Quelle: FAZ vom 24. Mai 2006). Eine konkrete Gefahr ist bei einer Sachlage gegeben, bei der das Eintreten einer Störung innerhalb eines nach der Lebenserfahrung vernünftigerweise in Betracht zu ziehenden Zeitraums mindestens so wahrscheinlich ist wie ihr Ausbleiben.

2

Absatz 1 Nummer 1 erfaßt Straftaten gegen das Schutzgut der Sicherheit des Staates, während Nummer 2 Straftaten zusammenfaßt, die sich gegen die Rechtsgüter Leib, Leben und Freiheit richten. Ob die Straftaten im In- oder Ausland begangen werden sollen, ist dabei unerheblich, da die Polizei nach § 1 Absatz 1 Nummer 1 unter anderem die Aufgabe hat, solche Straftaten zu verhüten, die zwar im Ausland begangen werden, aber nach Maßgabe der §§ 4 ff StGB im Inland strafbar sind. Das Gesetz verlangt darüber hinaus, daß tatsächliche Anhaltspunkte die Annahme rechtfertigen, daß die Übermittlung der Daten zur Verhütung der Straftaten erforderlich ist. Um „tatsächliche Anhaltspunkte“ bejahen zu können, muß nicht ein bestimmter Sachverhalt nachgewiesen sein. Vielmehr genügt es, wenn es nach der polizeilichen Erfahrung als möglich erscheint, daß dieser Sachverhalt vorliegen könnte und hierfür bestimmte Indizien sprechen.

3

Die Polizei kann nach Absatz 2 nur die Herausgabe bestimmter, vorher festgelegter Daten verlangen. Die Selektion der Datenbestände und das Herausfiltern der benötigten Daten aus einem Datenbestand obliegt der ersuchten Stelle. Die Polizei bekommt somit grundsätzlich nicht alle Daten, die bei der anderen Stelle vorhanden sind. Eine Ausnahme hiervon läßt Absatz 2 Satz 3 für den Fall zu, daß das Herausfiltern nicht mit vertretbarem Aufwand möglich ist. In diesem Fall dürfen die zusätzlich übermittelten Daten nicht verwertet werden. Absatz 2 Satz 2 2. Halbsatz schließt die Übermittlung von Daten aus, die einem Berufs- oder besonderen

Amtsgeheimnis unterliegen. Die Verweisung auf § 10 HmbSOG bezieht sich auf den Entschädigungsanspruch der in Anspruch genommenen Stellen. Die Absätze 3 bis 5 enthalten die der Bedeutung dieser Maßnahme angemessenen verfahrensrechtlichen Sicherungen. Insbesondere darf die Maßnahme nur durch den zuständigen Präses oder Staatsrat angeordnet werden.

§ 24 Berichtigen, Löschen und Sperren von Daten

(1) Personenbezogene Daten sind unverzüglich zu berichtigen, wenn sie unrichtig sind. Sind Daten in nichtautomatisierten Dateien oder in Akten zu berichtigen, reicht es aus, in geeigneter Weise kenntlich zu machen, zu welchem Zeitpunkt und aus welchem Grund diese Daten unrichtig waren oder geworden sind. Bestreitet der Betroffene die Richtigkeit gespeicherter Daten und lässt sich weder die Richtigkeit noch die Unrichtigkeit feststellen, sind die Daten entsprechend zu kennzeichnen.

(2) In Dateien suchfähig gespeicherte personenbezogene Daten sind zu löschen und die dazugehörigen, zu den Personen suchfähig angelegten Akten sind zu vernichten, wenn

1. **dies durch dieses Gesetz bestimmt ist,**
2. **ihre Speicherung unzulässig ist oder**
3. **bei der zu bestimmten Fristen oder Terminen vorzunehmenden Überprüfung oder aus Anlass einer Einzelfallbearbeitung festgestellt wird, dass ihre Kenntnis für die speichernde Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist.**

In Dateien nicht suchfähig gespeicherte Daten sind unter den Voraussetzungen der Nummern 1 bis 3 zu löschen, soweit die Speicherung festgestellt wird. Andere als die in Satz 1 genannten Akten sind nach Ablauf der jeweiligen Aufbewahrungsfrist oder bei unzulässiger Speicherung aller in ihnen enthaltenen Daten zu vernichten.

(3) Die Vernichtung von Akten ist bei Vorliegen der Voraussetzungen nach Absatz 2 Satz 1 Nummer 3 nur durchzuführen, wenn die gesamte Akte für die Aufgabenerfüllung nicht mehr erforderlich ist, es sei denn, dass der Betroffene die Vernichtung von Teilen der Akte verlangt und die weitere Speicherung ihn in unangemessener Weise beeinträchtigt. Soweit hiernach eine Vernichtung nicht in Betracht kommt, sind die Daten zu sperren und mit einem Sperrvermerk zu versehen.

(4) Löschung und Vernichtung unterbleiben, wenn

1. **Grund zu der Annahme besteht, dass dadurch schutzwürdige Belange des Betroffenen beeinträchtigt würden,**
2. **Daten, die nach Absatz 2 Nummern 1 und 2 zu löschen oder zu vernichten wären, in einem Verfahren, das den Anlass der Erhebung oder weiteren Verarbeitung dieser Daten betrifft, zur Behebung einer bestehenden Beweisnot unerlässlich sind,**
3. **die Nutzung der Daten für ein bestimmtes Forschungsvorhaben erforderlich ist.**

In diesen Fällen sind die Daten zu sperren und mit einem Sperrvermerk zu versehen. Sie dürfen nur zu den in Satz 1 genannten Zwecken oder sonst mit Einwilligung des Betroffenen genutzt werden.

(5) Stellt die Polizei fest, dass unrichtige oder nach Absatz 2 Satz 1 Nummer 2 zu löschende Daten übermittelt worden sind, ist dem Empfänger die

Berichtigung oder Löschung mitzuteilen, es sei denn, dass die Mitteilung für die Beurteilung der Person oder des Sachverhaltes nicht oder nicht mehr wesentlich ist.
(6) Anstelle der Löschung und Vernichtung in den Fällen des Absatzes 2 Satz 1 Nummer 3 können die Datenträger an das zuständige staatliche Archiv abgegeben werden, soweit archivrechtliche Regelungen dies vorsehen.

1

Absatz 1 entspricht § 19 Absatz 1 des Hamburgischen Datenschutzgesetzes. Absatz 2 beschränkt zunächst die Löschungs- und Vernichtungspflicht auf suchfähig gespeicherte personenbezogene Daten und die dazugehörigen zu den Personen suchfähig angelegten Akten. Die Differenzierung zwischen suchfähig und nicht suchfähig gespeicherten Daten trägt der Tatsache Rechnung, daß die in anderer Form gespeicherten Daten in der Regel nur mit unverhältnismäßigem Aufwand auffindbar sind und hierdurch in der Regel auch keine schutzwürdigen Interessen Betroffener berührt werden. Absatz 2 Satz 2 sieht daher nur eine Löschungspflicht vor, wenn die Speicherung z.B. anläßlich einer Sachbearbeitung im Einzelfall festgestellt wird.

2

Die Regelung in den Absätzen 3, 4 und 6 entspricht dem Hamburgischen Datenschutzgesetz. Absatz 4 stellt klar, daß Daten, die ursprünglich unzulässig gespeichert wurden oder deren Aufbewahrungsfrist abgelaufen ist, nicht gelöscht oder vernichtet werden dürfen, wenn die Angaben im Rahmen eines schwebenden Verwaltungs- oder Gerichtsverfahrens (einschließlich der Geltendmachung von Schadensersatzansprüchen) noch benötigt werden. Absatz 4 Nummer 3 hat ebenfalls nur deklaratorische Bedeutung. Die Frage, unter welchen Voraussetzungen polizeiliche Daten ftir wissenschaftliche Zwecke genutzt werden dürfen, ergibt sich aus dem allgemeinen Datenschutzrecht.

3

Nach Absatz 5 ist die Polizei verpflichtet, wenn sie im Zeitpunkt der Übermittlung unrichtige oder nach Absatz 2 Satz 1 Nummer 2 zu löschende personenbezogene Daten übermittelt hat, den Empfänger hiervon nachträglich zu unterrichten. Dies setzt zunächst voraus, daß der Empfänger noch bekannt ist. Die Polizei wird durch diese Bestimmung jedoch nicht verpflichtet, Datenübermittlungen zu protokollieren, um alle Empfänger von Datenübermittlungen nachträglich von Veränderungen unterrichten zu können. Ferner bedarf es keiner Mitteilung, wenn das Datum für die Beurteilung einer Person oder eines Sachverhaltes nicht oder nicht mehr wesentlich ist. Diese Einschränkung liegt auch im Interesse des Betroffenen, da in der Regel davon ausgegangen werden kann, daß eine eventuelle Unrichtigkeit entscheidungserheblicher Daten frühzeitig festgestellt wird. Andererseits könnte eine nachträgliche Mitteilung der Polizei auch den Betroffenen belasten, weil hierdurch offenkundig wird, daß die Polizei nach wie vor über ihn Daten gespeichert hat.

§ 25 Auskunft an den Betroffenen
Dem Betroffenen ist nach Maßgabe von § 18 des Hamburgischen Datenschutzgesetzes Auskunft zu erteilen.

Voraussetzungen, Umfang und Grenzen der Auskunftserteilung sind bereits abschließend im Hamburgischen Datenschutzgesetz geregelt. Da es sich um ein bedeutsames Schutzrecht für den Betroffenen handelt, wird es an dieser Stelle besonders hervorgehoben.

§ 26 Errichtungsanordnungen für Dateien
(1) Für jede Datei, für die nach § 9 Hamburgisches Datenschutzgesetz eine Verfahrensbeschreibung zu fertigen ist und die der Erfüllung von Aufgaben nach diesem Gesetz dient, sind in einer Anordnung festzulegen
1. ihr Zweck, ihre Bezeichnung und Rechtsgrundlage,
2. die Personen, über die Daten gespeichert werden dürfen,
3. die Art der Daten,
4. die Zugangsberechtigung,
5. die Voraussetzungen, unter denen in der Datei verarbeitete Daten an welche Empfänger und in welchem Verfahren übermittelt werden,
6. Prüfungstermine oder Speicherfristen nach § 15 in Verbindung mit § 16 Absätze 2 und 3,
7. die Voraussetzungen, unter denen dem Betroffenen Auskunft erteilt wird,
8. technische und organisatorische Maßnahmen nach § 8 des Hamburgischen Datenschutzgesetzes.
(2) Die Errichtung von Dateien wird durch den Polizeipräsidenten angeordnet. Dem Hamburgischen Datenschutzbeauftragten soll vor Erlass der Anordnungen Gelegenheit zur Stellungnahme gegeben werden. Die vorherige Beteiligung kann unterbleiben, wenn die Errichtung besonders eilbedürftig ist oder die Errichtung der Datei mit keinen besonderen rechtlichen, technischen oder organisatorischen Problemen verbunden ist.
(3) Die Polizei prüft alle vier Jahre die Notwendigkeit der Weiterführung oder Änderung der Dateien. Die Überprüfung ist aktenkundig zu machen.

1

Die Errichtungsanordnung ist eine besondere Form der Dateibeschreibung, für die allerdings besondere Verfahrensregelungen gelten. Zweck einer Errichtungsanordnung ist zum einen die Eigenkontrolle der Polizei und zum anderen die fachliche Steuerung ihrer Tätigkeit durch die mit der Aufsicht über die Polizei betrauten Stellen. Insoweit gehört der Erlaß von Errichtungsanordnungen zu den vom Bundesverfassungsgericht geforderten verfahrensrechtlichen Vorkehrungen zur Sicherung des Rechts auf informationelle Selbstbestimmung. Der Inhalt der Errichtungsanordnung entspricht dem Inhalt einer Dateibeschreibung. Insbesondere werden hierin die in den §§ 15 und 16 enthaltenen unbestimmten Rechtsbegriffe bzw. der Grundsatz der Erforderlichkeit näher konkretisiert und die Prüffristen für einzelne Dateien festgelegt.

2

Die Entscheidung über die Errichtung von Dateien ist dem Polizeipräsidenten vorbehalten. Hierdurch soll die besondere Bedeutung dieser Entscheidung hervorgehoben werden. Ferner ist nach Absatz 2 der Hamburgische Datenschutzbeauftragte beim Erlaß neuer Errichtungsanordnungen zu beteiligen. Auf eine vorherige Abstimmung kann nur verzichtet werden, wenn die Einrichtung einer neuen Datei besonders eilbedürftig ist. Außerdem kann auf die Beteiligung in Bagatellfällen oder in Fällen, in denen bereits eine gleichartige Datei besteht, verzichtet werden. Die Pflicht zur nachträglichen Unterrichtung des Hamburgischen Datenschutzbeauftragten bleibt hierdurch unberührt. Die Überprüfung nach Absatz 3 bezieht sich nicht auf die einzelnen in einer Datei gespeicherten Daten, sondern auf die Notwendigkeit der Datei selbst.

§ 27 Automatisierte Dateien und Verfahren, Datenverbund

(1) Die Einrichtung automatisierter Dateien ist nur zulässig, wenn das öffentliche Interesse an der Einrichtung gegenüber möglichen Gefahren für schutzwürdige Belange der Betroffenen überwiegt. Durch die Automatisierung darf keine unangemessene Verkürzung oder Verzerrung des Sachverhalts entstehen. Durch geeignete technische und organisatorische Maßnahmen ist insbesondere sicherzustellen, dass der Abruf der Daten nur den Bediensteten möglich ist, die hierfür im Einzelfall zuständig sind. Neben den nach § 8 Absatz 2 Hamburgisches Datenschutzgesetz zu treffenden Maßnahmen zur Datensicherung sind Maßnahmen zu treffen, die eine stichprobenweise Kontrolle der Zulässigkeit der Abrufe ermöglichen, soweit der damit verbundene Aufwand in einem angemessenen Verhältnis zur Schutzwürdigkeit der Daten steht.

(2) Für die Einrichtung eines Verfahrens, das der Polizei den automatisierten Abruf personenbezogener Daten aus einer von einer anderen öffentlichen Stelle geführten Datei ermöglicht, gilt § 11 Absatz 2 Hamburgisches Datenschutzgesetz entsprechend.

(3) Die zuständige Behörde darf zur Erfüllung von Aufgaben, die nicht nur örtliche Bedeutung haben, mit anderen Ländern und dem Bund einen Datenverbund vereinbaren, der eine automatisierte Datenübermittlung ermöglicht. In der Vereinbarung ist auch festzulegen, welcher Behörde die nach diesem Gesetz oder nach anderen Rechtsvorschriften bestehenden Pflichten einer speichernden Stelle obliegen. § 26 gilt entsprechend.

1

In Absatz 1 wird zum einen klargestellt, daß die Polizei in Erfüllung ihrer Aufgaben automatisierte Dateien einrichten darf. Darüber hinaus nennt diese Bestimmung die bei der Entscheidung über die EinrichtUng einer Datei gegeneinander abzuwägenden Gesichtspunkte. Hierdurch soll verdeutlicht werden, daß die Automation polizeilicher Dateiverarbeitung nicht ausschließlich unter der Zielsetzung der Verfahrensminimierung betrieben werden darf. Absatz 1 Satz 3 verlangt, daß die Zugangsberechtigung für automatisierte Dateien auf die hierfür jeweils zuständigen Mitarbeiter zu beschränken ist. Die Festlegung der Zugangsberechtigung für eine bestimmte Datei erfolgt in der jeweiligen Errichtungsanordnung (§ 26 Absatz 1 Nummer 4). Nach Absatz 1 Satz 4 ist darüber hinaus auch in geeigneten Fällen eine

stichprobenmäßige Protokollierung von Abrufen einzuführen. Eine lückenlose Protokollierung ist dagegen nicht vorgesehen, da dadurch neue datenschutzrechtliche Risiken eröffnet würden. Die Protokollierungsdaten unterliegen nach § 14 Absatz 2 einer strengen Zweckbindung.

2

Absatz 2 legt fest, daß ein unmittelbarer Zugriff der Polizei auf eine automatisierte Datei nur zulässig sein, wenn eine ausdrückliche Regelung in dem jeweiligen Fachgesetz enthalten ist. Eine allgemeine Regelung in einem Querschnittsgesetz oder in diesem Gesetz soll dagegen nicht ausreichend sein. Absatz 3 stellt klar, daß auch bei der Beteiligung Hamburgs an einer länderübergreifend oder bundesweit betriebenen Datei die Verfahrensregelungen dieses Gesetzes zu beachten sind. Nicht erfaßt sind von dieser Regelung Verbunddateien, die vom Bundeskriminalamt im Rahmen seiner Aufgaben bei der Zusammenarbeit des Bundes und der Länder im Bereich der Kriminalpolizei eingerichtet wurden. Die Einrichtung und der Betrieb dieser Dateien (insbesondere der Verbunddateien) richtet sich ausschließlich nach Bundesrecht (vgl. Artikel 73 Nummer 10 GG).

Vierter Abschnitt

Schlussbestimmung

§ 28 Einschränkung von Grundrechten
Durch dieses Gesetz werden die Grundrechte auf Freiheit der Person (Artikel 2 Absatz 2 Satz 2 des Grundgesetzes), auf Brief-, Post- und Fernmeldegeheimnis (Artikel 10 des Grundgesetzes) und auf Unverletzlichkeit der Wohnung (Artikel 13 des Grundgesetzes) eingeschränkt.

Die Vorschrift trägt dem Zitiergebot aus Artikel 19 Absatz 1 Satz 2 des Grundgesetzes Rechnung. Es geht hier insbesondere um die Befugnis, eine Person zum Zwecke der Identitätsfeststellung festzuhalten sowie um die Befugnisse zur Datenerhebung aus Wohnungen und zur präventiven Telekommunikationsüberwachung in den §§ 10a bis 10c, da die Maßnahmen den Schutzbereich der Artikel 2, 10 und 13 des Grundgesetzes berühren.