[Entwurf]

Gesetz zur Änderung des Bremischen Polizeigesetztes

Vom …

Der Senat verkündet das nachstehende, von der Bürgerschaft (Landtag) beschlossene Gesetz:

Artikel 1

Das Bremische Polizeigesetz in der Fassung der Bekanntmachung vom 6. Dezember 2001 (Brem.GBl. S. 441; 2002, S. 47 – 205-a-1), das zuletzt durch das Gesetz vom 14. November 2017 (Brem.GBl. S. 565) geändert worden ist, wird wie folgt geändert:

1. Die Inhaltsangabe wird wie folgt geändert:

   a) Nach der Angabe „§ 14a Wohnungsverweisung und Rückkehrverbot zum Schutz vor häuslicher Gewalt“ wird die Angabe „§ 14b Aufenthaltsanordnung und Kontaktverbot“ eingefügt.

   b) Nach der Angabe „§ 33 Datenerhebung durch den verdeckten Einsatz technischer Mittel“ werden folgende Angaben eingefügt:

      „§ 33a Telekommunikationsüberwachung und Eingriff in die Telekommunikation

      § 33b Quellen-Telekommunikationsüberwachung

      § 33c Verkehrsdatenerhebung und Standortermittlung

      § 33d Bestandsdatenerhebung

      § 33e Anordnung und Ausführung von Telekommunikationsmaßnahmen

      § 33f Elektronische Aufenthaltsüberwachung

      § 33g Schutz von Berufsgeheimnisträgern“

   c) Nach der Angabe „§ 83 Kosten“ werden folgende Angaben eingefügt:

      „Vierter Teil: Strafvorschriften

      § 84 Strafvorschriften“

   d) Die Wörter „Vierter Teil: Übergangs- und Schlussbestimmungen“ werden durch die Wörter „Fünfter Teil: Übergangs- und Schlussbestimmungen“ ersetzt.

   e) Die Angabe „§ 84“ wird durch die Angabe „§ 85“ ersetzt.

f) Die Angabe „§ 85“ wird durch die Angabe „§ 86“ ersetzt.

g) Die Angabe „§ 86“ wird durch die Angabe „§ 87“ ersetzt.

h) Die Angabe „§ 87“ wird durch die Angabe „§ 88“ ersetzt.

i) Die Angabe „§ 87a“ wird durch die Angabe „§ 89“ ersetzt.

j) Die Angabe „§ 88“ wird durch die Angabe „§ 90“ ersetzt.

2. § 2 wird wie folgt geändert:

a) Nach Nummer 5 wird folgende Nummer 6 eingefügt:

„6. terroristische Straftat:

a) eine Straftat nach §§ 89a, 89b, 89c, 91, 129a oder 129b des Strafgesetzbuches,

b) eine Straftat

aa) nach §§ 211, 212, 224, 226 oder 227 des Strafgesetzbuches,

bb) nach §§ 239a oder 239b des Strafgesetzbuches,

cc) nach §§ 303b, 305 oder 305a oder eine gemeingefährliche Straftat in den Fällen der §§ 306 bis 306c, des § 307 Absatz 1 bis 3, des § 308 Absatz 1 bis 4, des § 309, des § 310 Absatz 1 oder 2, der §§ 313, 314 oder 315 Absatz 1, 3 oder 4, des § 316b Absatz 1 oder 3, des § 316c Absatz 1 bis 3, des § 317 Absatz 1 oder des § 318 Absatz 1 des Strafgesetzbuches,

dd) nach § 328 Absatz 1 oder 2, § 330 Absatz 1 oder 2 oder § 330a Absatz 1 bis 3 des Strafgesetzbuches,

ee) nach § 19 Absatz 1 bis 3, § 20 Absatz 1 oder 2, § 20a Absatz 1 bis 3, jeweils auch in Verbindung mit § 21, oder nach § 22a Absatz 1 bis 3 des Gesetzes über die Kontrolle von Kriegswaffen,

ff) nach § 51 Absatz 1 bis 3 des Waffengesetzes,

gg) Völkermord nach § 6 des Völkerstrafgesetzbuches, ein Verbrechen gegen die Menschlichkeit nach § 7 des Völkerstrafgesetzbuches oder ein Kriegsverbrechen nach den §§ 8 bis 12 des Völkerstrafgesetzbuches,

bei Begehung im In- oder Ausland. Diese Straftat muss dazu bestimmt sein,

aa) die Bevölkerung auf erhebliche Weise einzuschüchtern,

bb) eine Behörde oder eine internationale Organisation rechtswidrig mit Gewalt oder durch Drohung mit Gewalt zu nötigen oder

cc) die politischen, verfassungsrechtlichen, wirtschaftlichen oder sozialen Grundstrukturen eines Staates, eines Landes oder einer internationalen Organisation zu beseitigen oder erheblich zu beeinträchtigen

und durch die Art ihrer Begehung oder ihre Auswirkungen einen Staat, ein Land oder eine internationale Organisation erheblich schädigen können."

b) Die bisherige Nummer 6 wird Nummer 7.

3. § 9 wird wie folgt gefasst:

§ 9

Einschränkung von Grundrechten

Durch dieses Gesetz werden die Grundrechte auf körperliche Unversehrtheit (Artikel 2 Absatz 2 Satz 1 des Grundgesetzes), Freiheit der Person (Artikel 2 Absatz 2 Satz 2 des Grundgesetzes), Unverletzlichkeit des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10 des Grundgesetzes), Freizügigkeit (Artikel 11 des Grundgesetzes) und Unverletzlichkeit der Wohnung (Artikel 13 des Grundgesetzes) eingeschränkt.

4. Nach § 14a wird folgender § 14b eingefügt:

„§ 14b

Aufenthaltsanordnung und Kontaktverbot

(1) Die Polizei kann zur Verhütung von terroristischen Straftaten einer Person untersagen, sich ohne Erlaubnis der zuständigen Polizeibehörde von ihrem Wohn- oder Aufenthaltsort oder aus einem bestimmten Bereich zu entfernen (Aufenthaltsgebot) oder sich an bestimmten Orten aufzuhalten (Aufenthaltsverbot), wenn

1. bestimmte Tatsachen die Annahme rechtfertigen, dass die betroffene Person innerhalb absehbarer Zeit auf eine zumindest ihrer Art nach konkretisierte Weise eine terroristische Straftat begehen wird, oder

2. das individuelle Verhalten der betroffenen Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb absehbarer Zeit eine terroristische Straftat begehen wird.

Soweit im Einzelfall ein besonderes Bedürfnis geltend gemacht wird, kann eine Ausnahme von dem Gebot oder Verbot nach Satz 1 zugelassen werden.

(2) Unter den Voraussetzungen des Absatzes 1 kann die Polizei zur Verhütung von terroristischen Straftaten einer Person auch den Kontakt mit bestimmten Personen oder Personen einer bestimmten Gruppe untersagen

(Kontaktverbot). Soweit im Einzelfall ein besonderes Bedürfnis geltend gemacht wird, kann eine Ausnahme von dem Verbot nach Satz 1 zugelassen werden.

(3) Gegenüber einer Person,

1. der nach § 8 in Verbindung mit § 7 Absatz 1 Nummer 1 oder 10 des Passgesetzes der Pass entzogen wurde,

2. gegen die eine Anordnung nach § 6 Absatz 7 des Personalausweisgesetzes in Verbindung mit § 7 Absatz 1 Nummer 1 oder 10 des Passgesetzes ergangen ist, oder

3. der die Ausreise nach § 46 Absatz 2 Satz 1 des Aufenthaltsgesetzes in Verbindung mit § 10 Absatz 1 Satz 1 und § 7 Absatz 1 Nummer 1 oder 10 des Passgesetzes untersagt wurde,

kann die Polizei den Aufenthalt in solchen örtlichen Bereichen untersagen, in denen eine Ausreise in das Ausland möglich ist, sofern bestimmte Tatsachen die Annahme rechtfertigen, dass die Person die Verbote nicht beachten wird. Entfällt die Maßnahme nach den Nummern 1 bis 3, so ist das Aufenthaltsverbot unverzüglich aufzuheben.

(4) Maßnahmen nach den Absätzen 1 bis 3 dürfen nur durch eine richterliche Entscheidung angeordnet werden. Bei Gefahr im Verzug kann die Anordnung durch die Behördenleitung getroffen werden. Im Übrigen gilt § 30 entsprechend. In diesem Fall ist die richterliche Entscheidung unverzüglich nachzuholen. Die Maßnahme ist zu beenden, wenn ihre Voraussetzungen nicht mehr vorliegen oder sie nicht innerhalb von drei Tagen durch eine richterliche Entscheidung bestätigt worden ist. Die Anordnung ist sofort vollziehbar. Für die richterliche Entscheidung ist das Amtsgericht zuständig, in dessen Bezirk die beantragende Polizeidienststelle ihren Sitz hat. Das Verfahren richtet sich nach den Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend.“

(5) Im Antrag sind anzugeben

1. die Person, gegen die sich die Maßnahme richtet mit Name und Anschrift,

2. Art, Umfang und Dauer der Maßnahme, einschließlich

   a) im Fall des Aufenthaltsgebots nach Absatz 1 einer Bezeichnung der Orte, von denen sich die Person ohne Erlaubnis der zuständigen Polizeibehörde nicht entfernen oder im Fall des Aufenthaltsverbots nach Absatz 1 oder 3, an denen sich die Person ohne Erlaubnis der zuständigen Polizeibehörde nicht aufhalten darf,

   b) im Fall des Kontaktverbots nach Absatz 2 der Personen oder Gruppe, mit denen oder mit der der betroffenen Person der Kontakt untersagt ist, soweit möglich, mit Name und Anschrift,

3. der Sachverhalt und

4. eine Begründung.

(6) Die Anordnung ergeht schriftlich. In ihr sind anzugeben

1. die Person, gegen die sich die Maßnahme richtet mit Name und Anschrift,

2. Art, Umfang und Dauer der Maßnahme, einschließlich

   a) im Fall der Aufenthaltsanordnung nach Absatz 1 oder 3 einer Bezeichnung der Orte, von denen sich die Person ohne Erlaubnis der zuständigen Polizeibehörde nicht entfernen oder an denen sich die Person ohne Erlaubnis der zuständigen Polizeibehörde nicht aufhalten darf,

   b) im Fall des Kontaktverbots nach Absatz 2 der Personen oder Gruppe, mit denen oder mit der der betroffenen Person der Kontakt untersagt ist, soweit möglich, mit Name und Anschrift,

3. die wesentlichen Gründe.

(7) Aufenthaltsanordnungen sowie Kontaktverbote sind auf den zur Verhütung von terroristischen Straftaten erforderlichen Umfang zu beschränken. Sie sind auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei Monate ist möglich, soweit ihre Voraussetzungen fortbestehen. Liegen die Voraussetzungen nicht mehr vor, ist die Maßnahme unverzüglich zu beenden.“

5. § 15 Absatz 1 Satz 1 wird wie folgt geändert:

   a) In Nummer 3 Buchstabe b wird der Punkt durch ein Komma ersetzt.

   b) In Nummer 4 wird der Punkt nach der Angabe „§ 14 a“ durch ein Komma ersetzt.

   c) Nach Nummer 4 wird folgende Nummer 5 angefügt:

   „5. um eine Aufenthaltsanordnung oder ein Kontaktverbot nach § 14b oder eine Anordnung zur elektronischen Aufenthaltsüberwachung nach § 33f durchzusetzen.“

6. § 29 wird wie folgt gefasst:

   a) Absatz 3 wird wie folgt gefasst:

   „(3) Der Polizeivollzugsdienst darf mittels Bildübertragung und -aufzeichnung offen und erkennbar folgende Orte und Anlagen beobachten:

   1. öffentlich zugängliche Orte, an denen vermehrt Straftaten begangen werden oder bei denen aufgrund der örtlichen Verhältnisse die Begehung von Straftaten besonders zu erwarten ist, wenn dies zur Erfüllung von Aufgaben nach § 1 Absatz 1 erforderlich ist,

   2. öffentlich zugängliche Anlagen und Flächen, an oder in denen sich in der Regel viele Personen gleichzeitig aufhalten, wie insbesondere

öffentliche Plätze, Haupteinstiegsbereiche des öffentlichen Nahverkehrs und Sport-, Versammlungs- oder Vergnügungsstätten an denen alleine die Vielzahl an Personen gleichzeitig vor Ort die Begehung von Straftaten erheblichen Umfangs oder Ausmaßes begünstigt,

3. wichtige Versorgungsanlagen sowie die unmittelbar im Zusammenhang mit dem Objekt stehenden Grün- oder Straßenflächen, an denen tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass an oder in ihnen terroristische Straftaten begangen werden,

4. bedeutende Amtsgebäude und Orte mit großer symbolischer Bedeutung sowie die unmittelbar im Zusammenhang mit dem Objekt stehenden Grün- oder Straßenflächen, an denen tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass an oder in ihnen terroristische Straftaten begangen werden.

Die Anordnung nach Satz 1 Nummer 2 bis 4 ist nur zulässig, soweit Tatsachen die Annahme rechtfertigen, dass Gefahren für Leib, Leben oder Freiheit bestehen; die Anordnung nach Satz 1 darf nicht gegen den Willen der Eigentümer dieser Objekte oder öffentlich zugänglichen Räume erfolgen. Die Anordnung der Bildübertragung und -aufzeichnung darf nur durch die Behördenleitung erfolgen. Im Übrigen gilt § 30 entsprechend. Regelmäßig innerhalb von zwei Jahren ist zu prüfen, ob die Voraussetzungen für die Anordnung weiter vorliegen. Die Orte sind nach Zustimmung des Senators für Inneres festzulegen. In geeigneter Weise ist vor Ort auf die Überwachung und die verantwortliche Stelle hinzuweisen.“

b) Absatz 4 wird wie folgt gefasst:

„(4) Die nach den Absätzen 1 und 2 hergestellten Aufzeichnungen und daraus gefertigte Unterlagen sind spätestens zwei Monate nach dem Zeitpunkt der Aufzeichnung zu löschen oder zu vernichten. Nach Absatz 3 Nummer 1 hergestellte Aufzeichnungen sind spätestens nach 48 Stunden zu löschen oder zu vernichten, soweit nicht die Aufbewahrung im Einzelfall zur Verfolgung von Straftaten oder von Ordnungswidrigkeiten weiterhin erforderlich ist. Nach Absatz 3 Nummer 2 bis 4 hergestellte Aufzeichnungen sind spätestens nach 30 Kalendertagen zu löschen oder zu vernichten, soweit nicht die Aufbewahrung im Einzelfall zur Verfolgung von Straftaten weiterhin erforderlich ist. Die Löschung ist zu protokollieren.“

7. Nach § 33 wird folgender § 33a eingefügt:

„§ 33a

Telekommunikationsüberwachung und Eingriff in die Telekommunikation

(1) Der Polizeivollzugsdienst darf durch die Überwachung und Aufzeichnung von Telekommunikation einschließlich der innerhalb des Telekommunikationsnetzes abgelegten Inhalte verdeckt Daten erheben

1. über die für eine Gefahr Verantwortlichen, wenn dies zur Abwehr einer gegenwärtigen Gefahr für den Bestand oder die Sicherheit des Bundes oder seiner Einrichtungen, eines Landes oder seiner Einrichtungen oder für Leib, Leben oder Freiheit einer Person erforderlich ist,

2. über Personen, wenn

   a) bestimmte Tatsachen die Annahme rechtfertigen, dass die betroffene Person innerhalb absehbarer Zeit auf eine zumindest ihrer Art nach konkretisierte Weise eine terroristische Straftat begehen wird, oder

   b) das individuelle Verhalten der betroffenen Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb absehbarer Zeit eine terroristische Straftat begehen wird,

   oder

3. über Kontakt- oder Begleitpersonen, soweit Tatsachen die Annahme rechtfertigen, dass

   a) sie für Personen nach Nummer 1 oder 2 bestimmte oder von diesen herrührende Mitteilungen entgegennehmen oder weitergeben oder

   b) die unter Nummer 1 oder 2 genannten Personen ihre Kommunikationseinrichtungen benutzen werden.

Datenerhebungen nach Satz 1 dürfen nur durchgeführt werden, wenn die polizeiliche Aufgabenerfüllung auf andere Weise aussichtslos oder wesentlich erschwert wäre.

(2) Die Überwachung ist unzulässig, soweit im Einzelfall aufgrund tatsächlicher Anhaltspunkte davon auszugehen ist, dass die Überwachung ausschließlich eine Kommunikation erfassen würde, die als höchstpersönlich dem Kernbereich privater Lebensgestaltung zuzurechnen ist oder dass in ein durch Berufsgeheimnis geschütztes Vertrauensverhältnis im Sinne der §§ 53 und 53a der Strafprozessordnung eingegriffen wird. Wird bei einer Maßnahme erkennbar, dass Gespräche geführt werden oder Nachrichten formuliert werden, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind oder in ein durch Berufsgeheimnis geschütztes Vertrauensverhältnis im Sinne der §§ 53 und 53a der Strafprozessordnung eingegriffen wird, ist die Maßnahme unverzüglich zu unterbrechen. Bestehen insoweit Zweifel, darf nur eine automatische Aufzeichnung fortgesetzt und die Nachricht zwecks Überprüfung durch ein Gericht gespeichert werden. Automatische Aufzeichnungen und Nachrichten nach Satz 3 sind unverzüglich dem anordnenden Gericht zur Entscheidung über die Verwertbarkeit oder Löschung der Daten vorzulegen. Nach einer Unterbrechung einer Aufzeichnung gemäß Satz 2 darf die Erhebung fortgesetzt werden, wenn zu erwarten ist, dass die Gründe, die zur Unterbrechung der Aufzeichnung geführt haben, nicht mehr vorliegen.

(3) Durch den Einsatz technischer Mittel dürfen unter den Voraussetzungen des Absatzes 1 Telekommunikationsverbindungen unterbrochen oder verhindert werden. Telekommunikationsverbindungen Dritter dürfen nur unterbrochen oder verhindert werden, wenn dies zur Abwehr einer unmittelbar bevorstehenden

Gefahr für den Bestand oder die Sicherheit des Bundes oder seiner Einrichtungen, eines Landes oder seiner Einrichtungen oder für Leib, Leben oder Freiheit einer Person erforderlich ist.

(4) Aufgrund der Anordnung einer Datenerhebung nach Absatz 1 oder einer Maßnahme nach Absatz 3 hat derjenige, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt (Diensteanbieter), nach Maßgabe der Regelungen des Telekommunikationsgesetzes und der darauf beruhenden Rechtsverordnungen zur technischen und organisatorischen Umsetzung von Überwachungsmaßnahmen der Polizei die Überwachung, Aufzeichnung, Unterbrechung oder Verhinderung von Telekommunikationsdienstleistungen zu ermöglichen.“

8. Nach § 33a wird folgender § 33b eingefügt:

„§ 33b

Quellen-Telekommunikationsüberwachung

(1) Zur Durchführung einer Maßnahme nach § 33a Absatz 1 darf durch den verdeckten Einsatz technischer Mittel in die vom Betroffenen genutzten informationstechnischen Systeme eingegriffen werden, wenn

1. durch technische Maßnahmen sichergestellt ist, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird, und

2. der Eingriff in das informationstechnische System notwendig ist, um die Überwachung und Aufzeichnung von Telekommunikation insbesondere auch in unverschlüsselter Form zu ermöglichen.

(2) Es ist technisch sicherzustellen, dass

1. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und

2. die vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden.

Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. § 33a Absatz 2 gilt entsprechend.

(3) Bei jedem Einsatz eines technischen Mittels sind zum Zwecke der Datenschutzkontrolle und der Beweissicherung zu protokollieren:

1. die Bezeichnung des technischen Mittels und der Zeitraum seines Einsatzes,

2. die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,

3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und

4. die Organisationseinheit, die die Maßnahmen durchführt.

Die Protokolldaten dürfen nur verwendet werden, um der betroffenen Person oder einer hierzu befugten öffentlichen Stelle oder einem Gericht die Prüfung zu ermöglichen, ob die Maßnahme nach Absatz 1 rechtmäßig durchgeführt worden ist. Sie sind bis zum Ablauf des auf die Speicherung folgenden Kalenderjahres aufzubewahren und sodann zu löschen, wenn sie für den in Satz 2 genannten Zweck nicht mehr erforderlich sind.

(4) Die Maßnahme darf sich nur gegen die für eine Gefahr Verantwortlichen richten. Sie darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden.“

9. Nach § 33b wird folgender § 33c eingefügt:

„§ 33c

Verkehrsdatenerhebung und Standortermittlung

(1) Der Polizeivollzugsdienst darf unter den Voraussetzungen des § 33a Absatz 1 Verkehrsdaten erheben.

(2) Die Erteilung einer Auskunft darüber, ob von einem Telekommunikationsanschluss Telekommunikationsverbindungen zu den in § 33a 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 § 33a Absatz 1 die Geräte- und Kartennummer,

2. zur Abwehr einer unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person der Standort eines aktiv geschalteten Mobilfunkendgerätes ermittelt werden.

(4) Eine Maßnahme nach Absatz 3 Nummer 1 ist nur zulässig, wenn die Voraussetzungen des § 33a Absatz 1 vorliegen und die Durchführung der Überwachungsmaßnahmen ohne die Geräte- und Kartennummer nicht möglich oder wesentlich erschwert wäre. Die Maßnahme nach Absatz 3 Nummer 2 ist nur dann zulässig, wenn die Ermittlung des Aufenthaltsortes auf andere Weise weniger erfolgversprechend 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. Über den Datenabgleich zur Ermittlung der gesuchten Geräte- und Kartennummer hinaus dürfen sie nicht verwendet werden und sind nach Beendigung der Maßnahme unverzüglich zu löschen.

(5) 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, die innerhalb des in der Anordnung festgelegten Zeitraums geführt werden, 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 dem Polizeivollzugsdienst unverzüglich oder innerhalb der in der Anordnung bestimmten Zeitspanne sowie auf dem darin bestimmten Übermittlungsweg zu übermitteln. Für die Entschädigung gilt § 23 des Justizvergütungs- und Entschädigungsgesetzes entsprechend.

(6) 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 Telekommunikationsdienstleistungen,

4. Endpunkte fest geschalteter Verbindungen, ihr Beginn und Ende nach Datum und Uhrzeit.“

10. Nach § 33c wird folgender § 33d eingefügt:

„§ 33d

Bestandsdatenerhebung

(1) Der Polizeivollzugsdienst darf von demjenigen, der geschäftsmäßig Telekommunikationsdienste oder Telemediendienste erbringt oder daran mitwirkt, Auskunft über Bestandsdaten über die für eine Gefahr Verantwortlichen oder der Begehung einer terroristischen Straftat Verdächtigen und unter den Voraussetzungen des § 7 über die dort genannten Personen verlangen, wenn dies zur Abwehr einer Gefahr für die öffentliche Sicherheit erforderlich ist. Bezieht sich das Auskunftsverlangen nach Satz 1 auf Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird, darf die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen.

(2) Die Auskunft nach Absatz 1 darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internet-Protokoll-Adresse sowie weiterer zur Individualisierung erforderlicher technischer Daten verlangt werden.

(3) Auf Grund eines Auskunftsverlangens nach Absatz 1 oder 2 hat derjenige, der geschäftsmäßig Telekommunikationsdienste oder Telemediendienste erbringt oder daran mitwirkt, die zur Auskunftserteilung erforderlichen Daten unverzüglich zu übermitteln. Für die Entschädigung der Diensteanbieter gilt § 23 des Justizvergütungs- und Entschädigungsgesetzes entsprechend.

(4) Für die Anordnung von Maßnahmen nach Absatz 1 Satz 2 und Absatz 2 gilt § 30 Satz 1 und 2 entsprechend. Für die Benachrichtigung von Personen, gegen die sich die Datenerhebung gerichtet hat, gilt in den Fällen des Absatzes 1 Satz 2 und des Absatzes 2 § 33 Absatz 5 entsprechend.

(5) Bestandsdaten im Sinne des Absatzes 1 oder 2 sind die nach §§ 95 und 111 des Telekommunikationsgesetzes erhobenen Daten.“

11. Nach § 33d wird folgender § 33e eingefügt:

„§ 33e Anordnung und Ausführung von Telekommunikationsmaßnahmen

(1) Maßnahmen nach §§ 33a, 33b und 33c bedürfen der richterlichen Anordnung. Bei Gefahr im Verzug können die Maßnahmen nach § 33a und § 33c durch die Behördenleitung angeordnet werden. Eine richterliche Bestätigung ist unverzüglich einzuholen. Die Maßnahme ist zu beenden, wenn ihre Voraussetzungen nicht mehr vorliegen oder sie nicht innerhalb von drei Tagen durch eine richterliche Entscheidung bestätigt worden ist; in diesem Fall sind die Datenaufzeichnungen unverzüglich zu vernichten. Das anordnende Gericht ist nach Beendigung der Maßnahme über deren Ergebnisse zu unterrichten. Für die richterliche Entscheidung ist das Amtsgericht zuständig, in dessen Bezirk die beantragende Polizeidienststelle ihren Sitz hat. Das Verfahren richtet sich nach den Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. Von einer Anhörung der betroffenen Person durch das Gericht und der Bekanntgabe der richterlichen Entscheidung an die betroffene Person ist abzusehen, wenn die vorherige Anhörung oder Bekanntgabe der Entscheidung den Zweck der Maßnahme gefährden würde. Die richterliche Entscheidung wird mit ihrer Bekanntgabe an die beantragende Stelle wirksam.

(2) Abweichend von Absatz 1 darf eine Maßnahme nach § 33c Absatz 3 Nummer 2, die allein auf die Ermittlung des Aufenthaltsortes einer vermissten, suizidgefährdeten oder hilflosen Person gerichtet ist, durch die Behördenleitung angeordnet werden. Im Übrigen gilt § 30 entsprechend.

(3) Anordnungen nach Absatz 1 müssen

1. den Namen und die Anschrift des Betroffenen, gegen den sie sich richten,

2. Art, Umfang und Dauer der Maßnahme,

3. die wesentlichen Gründe sowie

4. die Rufnummer oder eine andere Kennung seines Telekommunikationsanschlusses oder seines Endgerätes, wenn diese allein dem zu überwachenden Endgerät zuzuordnen ist,

enthalten oder das informationstechnische System bezeichnen. 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. Die Anordnung nach § 33a Absatz 1, § 33b Absatz 1, § 33c Absatz 1 oder § 33c Absatz 2 ist auf höchstens drei Monate zu befristen. Eine Verlängerung der Anordnungen nach § 33a Absatz 1, § 33b Absatz 1 oder § 33c Absatz 2 um jeweils nicht mehr als drei Monate ist zulässig, wenn die Voraussetzungen für die Maßnahme noch vorliegen. Die Anordnung nach § 33a Absatz 3 Satz 1 ist auf höchstens zwei Wochen, die Anordnung nach § 33a Absatz 3 Satz 2 auf höchstens zwei Tage zu befristen.

(4) Die durch eine Maßnahme nach Absatz 1 erlangten personenbezogenen Daten sind besonders zu kennzeichnen. Sie dürfen nur zu den Zwecken verwendet werden, zu denen sie erhoben wurden. Zu Zwecken der Strafverfolgung dürfen sie verwendet werden, wenn sie nach den Vorschriften der Strafprozessordnung für diesen Zweck hätten erhoben werden dürfen. Die Daten, die aufgrund einer Maßnahme nach § 33c Absatz 2 erlangt werden, dürfen über den Datenabgleich zur Ermittlung der gesuchten Geräte- und Kartennummer hinaus nicht verwendet werden. Daten bei denen sich nach der Auswertung herausstellt, dass sie dem Kernbereich privater Lebensgestaltung oder einem Vertrauensverhältnis mit Berufsgeheimnisträgern zuzuordnen sind, dürfen nicht verwendet werden. Daten, die keinen unmittelbaren Bezug zu den der Anordnung zugrunde liegenden Gefahren haben, dürfen nicht verwendet werden, es sei denn, ihre Verwendung ist zur Abwehr einer anderweitigen unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person oder zur Strafverfolgung unter der Voraussetzung von Satz 3 erforderlich.

(5) Personen, gegen die sich die Datenerhebungen nach §§ 33a bis 33d richteten oder die von ihnen sonst betroffen wurden, sind nach Beendigung der Maßnahme darüber zu unterrichten, sobald dies ohne Gefährdung des Zwecks der Datenerhebung geschehen kann. § 33 Absatz 5 Satz 2 bis 5 gilt entsprechend.

(6) Sind die aufgrund einer Maßnahme nach Absatz 1 erlangten Daten zur Aufgabenerfüllung nicht mehr erforderlich, sind sie zu löschen. Die Löschung ist zu protokollieren, dieses Protokoll bis zum Ablauf des auf die Löschung folgenden Kalenderjahres aufzubewahren und sodann zu löschen. Die Löschung der Daten unterbleibt, soweit die Daten für eine Mitteilung an den Betroffenen nach § 33 Absatz 5 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. Daten, die dem Kernbereich privater Lebensgestaltung oder einem Vertrauensverhältnis mit Berufsgeheimnisträgern zuzuordnen sind, sind unverzüglich zu löschen. Daten, die keinen unmittelbaren Bezug zu den der Anordnung zugrunde liegenden Gefahren haben, sind zu löschen, es sei denn, ihre Verwendung ist zur Abwehr einer anderweitigen unmittelbar bevorstehenden Gefahr für Leib, Leben oder

Freiheit einer Person oder zur Strafverfolgung unter der Voraussetzung von Absatz 4 Satz 3 erforderlich.“

12. Nach § 33e wird folgender § 33f eingefügt:

„§ 33f

Elektronische Aufenthaltsüberwachung

(1) Die Polizei kann eine Person dazu verpflichten, ein technisches Mittel, mit dem der Aufenthaltsort dieser Person elektronisch überwacht werden kann, ständig in betriebsbereitem Zustand am Körper bei sich zu führen und dessen Funktionsfähigkeit nicht zu beeinträchtigen, wenn

1. bestimmte Tatsachen die Annahme rechtfertigen, dass diese Person innerhalb absehbarer Zeit auf eine zumindest ihrer Art nach konkretisierte Weise eine terroristische Straftat begehen wird, oder

2. das individuelle Verhalten dieser Person die konkrete Wahrscheinlichkeit dafür begründet, dass sie innerhalb absehbarer Zeit eine terroristische Straftat begehen wird,

um diese Person durch die Überwachung und die Datenverwendung von der Begehung dieser Straftaten abzuhalten.

(2) Dieselbe Befugnis steht der Polizei zu gegenüber einer Person, der

1. nach § 8 in Verbindung mit § 7 Absatz 1 Nummer 1 oder 10 des Passgesetzes der Pass entzogen wurde oder

2. gegen die eine Anordnung nach § 6 Absatz 7 des Personalausweisgesetzes in Verbindung mit § 7 Absatz 1 Nummer 1 oder 10 des Passgesetzes ergangen ist oder

3. der die Ausreise nach § 46 Absatz 2 Satz 1 des Aufenthaltsgesetzes in Verbindung mit § 10 Absatz 1 Satz 1 und § 7 Absatz 1 Nummer 1 oder 10 des Passgesetzes untersagt wurde,

um diese Person durch die Überwachung und die Datenverwendung von der Ausreise abzuhalten, sofern bestimmte Tatsachen die Annahme rechtfertigen, dass die Person die Ausreise beabsichtigt.

(3) Die Polizei kann mit Hilfe des von der verantwortlichen Person mitgeführten technischen Mittels automatisiert Daten über deren Aufenthaltsort sowie über etwaige Beeinträchtigungen der Datenerhebung erheben und speichern. Soweit es technisch möglich ist, ist sicherzustellen, dass innerhalb der Wohnung der betroffenen Person keine über den Umstand ihrer Anwesenheit hinausgehenden Aufenthaltsdaten erhoben werden. Werden innerhalb der Wohnung der betroffenen Person über den Umstand ihrer Anwesenheit hinausgehende Aufenthaltsdaten erhoben, dürfen diese nicht verwendet werden. Entsprechendes gilt, soweit durch die Datenerhebung nach

Satz 1 der Kernbereich privater Lebensgestaltung betroffen ist. Daten nach Satz 3 und 4 sind unverzüglich nach ihrer Kenntnisnahme zu löschen. Die Tatsache ihrer Kenntnisnahme und Löschung ist zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist frühestens nach Abschluss der Datenschutzkontrolle und spätestens nach 24 Monaten zu löschen. Daten nach Satz 1 dürfen ohne Einwilligung der betroffenen Person nur verarbeitet werden, soweit dies erforderlich ist für die folgenden Zwecke:

1. zur Verhütung oder zur Verfolgung von terroristischen Straftaten,

2. zur Feststellung von Verstößen gegen Aufenthaltsge- und -verbote nach § 14b Absatz 1 und Kontaktverbote nach § 14b Absatz 2,

3. zur Verfolgung einer Straftat nach § 84,

4. zur Abwehr einer erheblichen gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person oder

5. zur Aufrechterhaltung der Funktionsfähigkeit der technischen Mittel.

Die Daten sind gegen unbefugte Kenntnisnahme und Verarbeitung besonders zu sichern. Eine Zweckänderung ist festzustellen und zu dokumentieren.

(4) Die in Absatz 3 Satz 1 genannten Daten sind spätestens zwei Monate nach Beendigung der Maßnahme zu löschen, soweit sie nicht für die in Absatz 3 Satz 9 genannten Zwecke verwendet werden. Bei jedem Abruf der Daten sind der Zeitpunkt, die abgerufenen Daten, die bearbeitende Person und der Grund des Abrufs samt Geschäftszeichen zu protokollieren. Die durch eine Maßnahme nach Absatz 1 und 2 erhobenen Daten sind besonders zu kennzeichnen und gegen unbefugte Kenntnisnahme und Verwendung außerhalb des Zwecks der Maßnahme besonders zu sichern. Die Maßnahmen sind zu protokollieren. Aus den Protokollen muss der für die Maßnahmen und Datenerhebungen Verantwortliche, Ort, Zeitpunkt, Dauer, Zweck und wesentliches Ergebnis der Maßnahme sowie Angaben über die weitere Verarbeitung der erhobenen Daten ersichtlich sein. Die Protokolle werden ausschließlich zur Überprüfung der Rechtmäßigkeit der Datenverarbeitung, der Eigenüberwachung sowie der Sicherstellung der Integrität und Sicherheit der personenbezogenen Daten verwendet. Die verantwortliche Stelle sowie der Auftragsverarbeiter stellen die Protokolle der Aufsichtsbehörde auf Anforderung zur Verfügung. Die Protokolldaten sind spätestens nach 24 Monaten zu löschen.

(5) Eine Maßnahme nach Absatz 1 und 2 darf nur durch eine richterliche Entscheidung angeordnet werden, bei Gefahr im Verzug auch durch die Behördenleitung; im Übrigen gilt § 30 entsprechend. In diesem Fall ist unverzüglich eine richterliche Bestätigung der Maßnahme einzuholen. Die Anordnung tritt außer Kraft, wenn sie nicht innerhalb von drei Tagen durch eine richterliche Entscheidung bestätigt worden ist.

(6) In dem Antrag sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, mit Name und Anschrift,

2. Art, Umfang und Dauer der Maßnahme sowie die Angabe, ob gegenüber der Person, gegen die sich die Maßnahme richtet, eine Aufenthaltsanordnung, ein Kontaktverbot oder eine Maßnahme nach Absatz 2 besteht,

3. der Sachverhalt sowie

4. eine Begründung.

(7) Die Anordnung ergeht schriftlich. In ihr sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, mit Name und Anschrift,

2. Art, Umfang und Dauer der Maßnahme sowie

3. die wesentlichen Gründe.

(8) Die Anordnung ist sofort vollziehbar und auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei Monate ist möglich, soweit die Anordnungsvoraussetzungen fortbestehen. Liegen die Voraussetzungen der Anordnung nicht mehr vor, ist die Maßnahme unverzüglich zu beenden. Für die richterliche Entscheidung ist das Amtsgericht zuständig, in dessen Bezirk die beantragende Polizeidienststelle ihren Sitz hat. Das Verfahren richtet sich nach den Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend.“

13. Nach § 33f wird folgender § 33g eingefügt:

„§ 33g

Schutz von Berufsgeheimnisträgern

(1) Maßnahmen nach §§ 33a bis 33d und 33f, die sich gegen eine in § 53 Absatz 1 Satz 1 Nummer 1, 2, 3 oder 4 der Strafprozessordnung genannte Person richten und voraussichtlich Erkenntnisse erbringen würden, über die diese Person das Zeugnis verweigern dürfte, sind unzulässig. Dennoch erlangte Erkenntnisse dürfen nicht verwertet werden. Aufzeichnungen hierüber sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren. Die Sätze 2 bis 4 gelten entsprechend, wenn durch eine Maßnahme nach §§ 33a bis 33d und § 33f, die sich nicht gegen eine in § 53 Absatz 1 Satz 1 Nummer 1, 2, 3 oder Nummer 4 der Strafprozessordnung genannte Person richtet, von einer dort genannten Person Erkenntnisse erlangt werden, über die sie das Zeugnis verweigern dürfte. Für Personen nach § 53 Absatz 1 Satz 1 Nummer 3 der Strafprozessordnung gelten die Sätze 1 bis 5 nur, soweit es sich um Rechtsanwälte oder Kammerrechtsbeistände handelt.

(2) Soweit durch eine Maßnahme nach §§ 33a bis 33d oder § 33f eine in § 53 Absatz 1 Satz 1 Nummer 3, 3a und 3b oder Nummer 5 der Strafprozessordnung genannte Person betroffen wäre und dadurch voraussichtlich Erkenntnisse erlangt würden, über die diese Person das Zeugnis verweigern dürfte, ist dies im Rahmen der Prüfung der Verhältnismäßigkeit unter Würdigung des öffentlichen

Interesses an den von dieser Person wahrgenommenen Aufgaben und des Interesses an der Geheimhaltung der dieser Person anvertrauten oder bekannt gewordenen Tatsachen besonders zu berücksichtigen. Soweit hiernach geboten, ist die Maßnahme zu unterlassen oder, soweit dies nach der Art der Maßnahme möglich ist, zu beschränken. Für Personen nach § 53 Absatz 1 Satz 1 Nummer 3 der Strafprozessordnung gelten die Sätze 1 und 2 nur, soweit es sich nicht um Rechtsanwälte oder Kammerrechtsbeistände handelt.

(3) Die Absätze 1 und 2 gelten entsprechend, soweit die in § 53a der Strafprozessordnung genannten Personen das Zeugnis verweigern dürften.

(4) Die Absätze 1 bis 3 gelten nicht, sofern Tatsachen die Annahme rechtfertigen, dass die zeugnisverweigerungsberechtigte Person für die Gefahr verantwortlich ist.“

14. Nach § 83 wird folgende Überschrift eingefügt:

„Vierter Teil: Strafvorschriften“

15. Nach der Überschrift „Vierter Teil: Strafvorschriften“ wird folgender § 84 eingefügt:

„§ 84

Strafvorschriften

(1) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer

1. einer gerichtlichen Anordnung nach § 14b Absatz 1 bis 3 zuwiderhandelt und dadurch den Zweck der Anordnung gefährdet oder

2. einer gerichtlichen Anordnung nach § 33f Absatz 1 oder 2 zuwiderhandelt und dadurch die kontinuierliche Feststellung seines Aufenthaltsortes durch die Polizei verhindert.

(2) Die Tat wird nur auf Antrag der Polizeibehörde verfolgt, die die Maßnahme angeordnet oder beantragt hat.“

16. Die Überschrift „Vierter Teil: Übergangs- und Schlussbestimmungen“ wird ersetzt durch die Überschrift „Fünfter Teil: Übergangs- und Schlussbestimmungen“

17. Die Bezeichnung „§ 84“ wird durch die Bezeichnung „§ 85“ ersetzt.

18. Die Bezeichnung „§ 85“ wird durch die Bezeichnung „§ 86“ ersetzt.

19. Die Bezeichnung „§ 86“ wird durch die Bezeichnung „§ 87“ ersetzt.

20. Die Bezeichnung „§ 87“ wird durch die Bezeichnung „§ 88“ ersetzt.

21. Die Bezeichnung „§ 87a“ wird durch die Bezeichnung „§ 89“ ersetzt.

22. Die Bezeichnung „§ 88“ wird durch die Bezeichnung „§ 90“ ersetzt.

Artikel 2

Dieses Gesetz tritt am Tage nach seiner Verkündung in Kraft.

Bremen, Der Senat

Begründung

A. Allgemeines

Seit Jahren befindet sich Deutschland in einer Phase mit dauerhaft erhöhter Anschlagsgefahr. In den zurückliegenden Jahren hat sich diese abstrakte Gefahr mehrfach konkretisiert. Die Freie Hansestadt Bremen ist nach wie vor ein Zentrum der salafistischen und radikalislamistischen Szene in Deutschland. Das Landesamt für Verfassungsschutz zählt inzwischen mehrere Hundert Salafisten in Bremen. Unter ihnen befinden sich viele, die auch mit Mitteln der Gewalt dazu bereit sind, die freiheitliche demokratische Grundordnung anzugreifen. Gefahren im Bereich der politisch motivierten Kriminalität gehen aber auch von links- oder rechtsextremistischen militanten Gruppen aus. Die Antwort auf diese Herausforderungen liegt im Dreiklang aus Prävention, Gefahrenabwehr und konsequenter Strafverfolgung. Der vorliegende Gesetzesentwurf setzt an allen drei Anknüpfungspunkten an. Der Schwerpunkt liegt in der Gefahrenvorsorge und -abwehr.

Es ist Aufgabe der Freien Hansestadt Bremen, ihre Bürgerinnen und Bürger vor Gefahren und Straftaten zu schützen. Das Gewaltmonopol gibt ihr hierzu das Recht, aber auch die Pflicht. Gleichzeitig hat sie die Grundrechte zu achten. D.h., sie muss einen rechtsstaatlichen Ausgleich zwischen Freiheit und Sicherheit schaffen. Die Sicherheit des Einzelnen und seine Freiheit stehen in einem engen Wechselspiel: Nur wenn die Bürgerinnen und Bürger ausreichend vor Gefahren geschützt werden, können sie sich nach ihren Vorstellungen und Fähigkeiten frei entfalten.

Um einen hohen Sicherheitsstandard insbesondere zum Schutz der überragenden Rechtsgüter Leib, Leben und Freiheit der Bürgerinnen und Bürger zu erreichen, müssen die Sicherheitsbehörden dazu in die Lage versetzt werden, diese überragenden Rechtsgüter zu verteidigen. Hierbei spielen technische Entwicklungen eine wichtige Rolle. Denn diese Entwicklungen werden vor allem von Kriminellen schnell aufgenommen und eingesetzt, um ihre Taten vorzubereiten, sich mit anderen Kriminellen abzustimmen und die Straftaten durchzuführen. Daher führen insbesondere Entwicklungen im technischen Bereich auch zum Anpassungsbedarf bei den Befugnissen der Sicherheitsbehörden. Neue oder erweiterte Befugnisse der Sicherheitsbehörden können allerdings auch zu gesteigerter Betroffenheit grundrechtlich geschützter Positionen führen. Es ist daher die Aufgabe des Gesetzgebers hier mit besonderem Augenmaß vorzugehen, um sowohl dem berechtigten Schutz der Rechtsgüter als auch der freien Entfaltung der Bürgerinnen und Bürger und ihrer Grundrechtsausübung Rechnung zu tragen.

In diesem Spannungsfeld stellen die Erscheinungsformen der schweren Kriminalität (insbesondere der internationale Terrorismus als Erscheinungsform der politisch motivierten Kriminalität und die Organisierte Kriminalität) die Sicherheitsbehörden vor besondere Herausforderungen. Die Bedrohungslage durch die politisch motivierte Kriminalität hat in den zurückliegenden Jahren stetig zugenommen. Insbesondere seit 2015 hat sich eine Vielzahl an politisch motivierten Straftaten durch islamistische Terroristen und sonstige Täter, mit Hass auf den Staat oder Religionsangehörige, in Europa und namentlich in Deutschland ereignet. Diese Taten hatten und haben erhebliche Auswirkungen auf das Leben vieler Menschen, das gesellschaftliche Zusammenleben und die Grundrechtsausübung der Bürgerinnen und Bürger. Zu nennen sind u. a.:

- der Anschlag auf die Redaktionsbüros der Satirezeitschrift „Charlie Hebdo“ und auf einen jüdischen Supermarkt in Paris im Januar 2015 (17 Tote),
- die Messerattacke auf drei Soldaten in Nizza im Februar 2015, die Anschlagserie auf Besucherinnen und Besucher einer Konzerthalle sowie von Bars und Restaurants in Paris im November 2015 (130 Tote, 350 Verletzte),
- der Angriff auf einen Bundespolizisten im Hauptbahnhof in Hannover im Februar 2015,

- die Absage des Fußballländerspiels Deutschland gegen die Niederlande in Hannover wegen konkreter Hinweise auf Bombenanschläge im Stadion und am Hauptbahnhof Hannover im November 2015,
- die Terroranschläge auf den Flughafen und auf Metrostationen in Brüssel im März 2016 (35 Tote, 300 Verletzte),
- der Sprengstoffanschlag auf ein Gebetshaus der Sikh in Essen im April 2016,
- das Lkw-Attentat in Nizza im Juli 2016 (86 Tote),
- der Sprengstoffanschlag in der Altstadt von Ansbach im Juli 2016 (15 Verletzte),
- das Lkw-Attentat auf den Weihnachtsmarkt in Berlin im Dezember 2016 (12 Tote, 50 Verletzte),
- der Pkw-Anschlag auf der Westminster-Brücke in London im März 2017 (4 Tote, 40 Verletzte),
- der Sprengstoffanschlag auf ein Konzert in Manchester im Mai 2017 (22 Tote)
- die Angriffe auf Passanten auf der London Bridge in London im Juni 2017 (8 Tote)
- die Messerattacke in Hamburg im Juli 2017 (1 Toter) und
- das Lkw-Attentat in Barcelona im August 2017 (14 Tote, 130 Verletzte).

Zudem wurden einige terroristische Straftaten verhindert bei denen Kriminelle u. a. Sturmgewehre und/oder Sprengstoffe einsetzen wollten, um möglichst vielen Menschen zu schaden.

Die bestehenden polizeilichen Befugnisse sind nicht ausreichend, um den durch diese Formen der Kriminalität ausgelösten Gefahren präventiv zu begegnen. Das Bremische Polizeigesetz muss den aktuellen Bedürfnissen einer effektiven Gefahrenabwehr angepasst werden. Der vorgelegte Gesetzesentwurf fügt Befugnisse in das Bremische Polizeigesetz ein, mit denen den aktuellen technischen Entwicklungen, vor allem im Bereich der Telekommunikation, besonders Rechnung getragen wird.

Zum Zwecke der Gefahrenabwehr werden Befugnisse

- zur Telekommunikationsüberwachung (§§ 33a und § 33b),
- zur Unterbrechung der Telekommunikation (§ 33a Abs. 3),
- zur Verkehrs- und Bestandsdatenauskunft (§§ 33c und 33d),
- zur Standortfeststellung von Mobilfunkgeräten (§§ 33c Absatz 3 und 5),
- zum bedarfsgerechten Ausbau der Videoüberwachung bei besonders schutzwürdigen öffentlichen Orten (§ 29 Absatz 3 und 4),
- zur elektronischen Aufenthaltsüberwachung (§ 33f)

sowie ergänzende Vorschriften in §§ 2 Nummer 6, 9, 14b, 33e und 33g sowie 84 in das Gesetz aufgenommen.

Der Polizeivollzugsdienst der Freien Hansestadt Bremen wird mit diesen Instrumenten in die Lage versetzt, insbesondere den Erscheinungsformen der Organisierten Kriminalität und der politisch motivierten Kriminalität effektiv entgegenzutreten. Diese Kriminalitätsbereiche sind geprägt von einer arbeitsteiligen Vorgehensweise, bei der einzelne Einheiten abgeschottet und unter Einsatz modernster Kommunikationstechnologie Straftaten mit erheblichen Auswirkungen auf die Betroffenen, die Gesellschaft und die freiheitliche demokratische Grundordnung vorbereiten und begehen. In der polizeilichen Praxis kommt es immer wieder zu Situationen, in denen strafprozessuale Maßnahmen (noch) nicht greifen und damit z. B. die Telekommunikationsüberwachung (TKÜ) oder Standortermittlung ausgeschlossen ist, obwohl sie aus gefahrenabwehrrechtlichen Gründen geboten erscheint.

Diese Situation trifft auch auf Fälle zu bei denen die Personen keine Straftat begehen, aber zu ihrem Schutz die Ermittlung ihres Standorts notwendig ist. Bei vermissten, hilflosen, demenzkranken oder suizidgefährdeten Personen kann die Standortermittlung mitunter das einzig wirksame Mittel darstellen, um unumkehrbare Schäden für Leib oder Leben zu verhindern.

Der technische Fortschritt und die damit einhergehende zunehmende Bedeutung digitaler Kommunikation lässt die ohnehin hohe gefahrenabwehrrechtliche Notwendigkeit dieser Ermittlungsbefugnisse weiter ansteigen. U. a. auch die massiven Übergriffe in der Silvesternacht vom 31.12.2015 auf den 01.01.2016 sowie in den nachfolgenden Wochen in mehreren deutschen Großstädten haben gezeigt, dass zur Bekämpfung dieser Gefahren der Einsatz von technischen Instrumenten, hier der Videoüberwachung, erforderlich ist, um Kriminelle abzuschrecken und frühzeitig eingreifen sowie im Einsatzfall erforderliche Maßnahmen besser steuern zu können.

Insbesondere zum Schutz des Grundrechts auf informationelle Selbstbestimmung darf der Polizeivollzugsdienst von den genannten Befugnissen nur zum Schutz sehr hochrangiger Rechtsgüter und nur in einem konkret festgelegten Verfahren mit klaren Zuständigkeiten Gebrauch machen. Die Einhaltung der Vorgaben wird daher entsprechend nach engen Maßstäben kontrolliert.

Ohne diese Befugnisse wäre die Sicherheitslage nicht nur in der Freien Hansestadt Bremen, sondern auch darüber hinaus betroffen. Die Bekämpfung der politisch motivierten Kriminalität (insbesondere islamistischer Terrorismus und Links- bzw. Rechtsterrorismus) erfordert nicht zuletzt wegen der vielen Reisebewegungen von Personen, die diesem Kriminalitätsphänomen zuzurechnen sind, sowie der überregionalen, zumeist internationalen Dimension, von Terrornetzwerken eine intensive Zusammenarbeit zwischen Bund und Ländern. Diese Zusammenarbeit besteht primär in einem Informationsaustausch. Darüber hinaus sind allerdings auch die Befugnisse darauf zu überprüfen, ob ein Gefälle zu anderen Bundesländern besteht. Eine effektive Gefahrenabwehr wird wesentlich erschwert oder gar vereitelt, wenn die polizeiliche Überwachung von Kriminellen mittels einer Maßnahme wegen eines Zuständigkeitswechsels infolge eines neuen Aufenthaltsortes aufgrund dort fehlender oder eingeschränkter Befugnisse nicht möglich ist.

Die in diesem Gesetz geregelten polizeilichen Befugnisse orientieren sich an gefahrenabwehrrechtlichen bundeseinheitlichen Empfehlungen sowie an Regelungen anderer Bundesländer oder des Bundes. Hierdurch soll gerade auch in Anbetracht der länderübergreifenden Kriminalitätsphänomene ein einheitlicher, hoher Standard der Gefahrenabwehr und -vorsorge sichergestellt werden. Der vorliegende Entwurf trägt dem Ansatz Rechnung, dass sich die Landesregelungen untereinander und die Landesregelungen auch den Bundesregelungen wieder stärker annähern, um so einheitlich den – insbesondere internationalen – Gefahren zu begegnen. Der Entwurf berücksichtigt die verfassungsrechtlichen Vorgaben zum Schutz der Grundrechte und hier insbesondere die Rechtsprechung des Bundesverfassungsgerichts zum sog. Bundeskriminalamtgesetz vom 20. April 2016 (1 BvR 966/09 u. a.).

B. Zu den einzelnen Vorschriften

Zu Artikel 1

Zu Nummer 1 – Anpassung der Inhaltsangabe

Aufgrund der Einfügung von neuen Paragraphen muss die Inhaltsübersicht entsprechend redaktionell angepasst werden.

Durch die Neuaufnahme von Strafvorschriften wird die Bildung eines weiteren Teils erforderlich.

Zu Nummer 2 – § 2 (Definition terroristische Straftat)

Die Norm beschreibt Straftaten, die sich aufgrund ihres Gepräges und ihrer Intensität auf die freiheitlich demokratische Grundordnung nur zum Teil mit den erheblichen Straftaten im Sinne von Nummer 5 decken. Die hier genannten Straftaten richten sich gegen die hochrangigen Rechtsgüter Leib, Leben oder Freiheit oder richten sich als gemeingefährliche Straftaten aufgrund ihrer Streubreite und Gefahren gegen diese Rechtsgüter oder den Bestand oder die Sicherheit des Bundes oder des Landes sowie seiner Einrichtungen.

Die Definition ist in Abgrenzung zu den erheblichen Straftaten in Nummer 5 erforderlich, da von den in Nummer 6 genannten terroristischen Straftaten eine gegenüber den erheblichen Straftaten gesteigerte Beeinträchtigung der höchsten Verfassungsgüter ausgeht – und zwar sowohl hinsichtlich der Anzahl der betroffenen Personen als auch der Intensität.

Durch die Aufnahme dieser Straftaten in § 2 Nummer 6 wird vermieden, dass in den §§ 14b, 29, 33a und 33f die hier genannten Straftaten jeweils aufgeführt werden müssen. Da zur Bekämpfung der terroristischen Straftaten im Sinne des § 2 Nummer 6 neue Instrumente in das Gesetz eingeführt werden und durch die Befugnisse eine höhere Beeinträchtigung von Freiheitsrechten im Einzelfall ausgehen kann, ist eine stärkere Unterscheidung der beiden Straftatenkataloge erforderlich.

Der Straftatenkatalog in § 2 Nummer 6 orientiert sich vor allem an den Straftaten nach § 129a Strafgesetzbuch und § 4 Bundeskriminalamtgesetz in seiner beschlossen Fassung, die am 25.05.2018 in Kraft tritt. Zusätzlich enthält dieser Katalog auch Vorschriften, die nicht in § 4 BKAG 2018 genannt werden. Hierdurch wird u. a. dem Umstand Rechnung getragen, dass die §§ 89a bis 89c, §§ 129a und 129b sowie §§ 310, 328 und 330 Strafgesetzbuch nach der Richtlinie (EU) 2017/541 des Europäischen Parlaments und des Rates vom 15.03.2017 zur Terrorismusbekämpfung und zur Ersetzung des Rahmenbeschlusses 2002/475/JI des Rates und zur Änderung des Beschlusses 2005/671/JI des Rates als terroristische Straftaten einzustufende Verhaltensweisen darstellen, zu deren Ahndung die Mitgliedstaaten angehalten sind. Dies gilt nach Artikel 13 dieser Richtlinie bereits schon für den Zeitraum vor der Tatbegehung. Aus Gründen der Gefahrenabwehr sind daher auch die in § 2 Nummer 6 Buchstabe b) genannten Straftaten des Strafgesetzbuches erfasst.

Zu Nummer 3 – § 9 (Einschränkung von Grundrechten)

Die Änderung trägt dem Zitiergebot aus Artikel 19 Absatz 1 Satz 2 Grundgesetz für die präventive Telekommunikationsüberwachung in den §§ 33a bis d Rechnung, da die Maßnahmen den Schutzbereich von Artikel 10 Grundgesetz berühren.

Da mit dem vorliegenden Gesetz bereits benannte Grundrechtseingriffe intensiviert oder auf andere Sachverhalte ausgeweitet werden können, werden die betroffenen Grundrechte erneut zitiert (vgl. BVerfG, Urteil vom 27.07.2005 – 1 BvR 668/04, juris Rn. 85 ff.).

Das Recht auf körperliche Unversehrtheit kann insbesondere durch die Ingewahrsamnahme nach § 15 Absatz 1 Satz 1 Nummer 5 sowie durch die elektronische Aufenthaltsüberwachung und das Anbringen des Signalgebers nach § 33f beeinträchtigt sein. Die Freiheit der Person und die Freizügigkeit werden ebenfalls durch diese Normen betroffen. Die Unverletzlichkeit des Brief-, Post- und Fernmeldegeheimnisses sowie die Unverletzlichkeit der Wohnung ist insbesondere durch die Regelungen in §§ 33a bis 33e und 33g betroffen. Die Unverletzlichkeit der Wohnung kann nach § 33f durch das Aufstellen der sog. Hauseinheit eingeschränkt sein.

Die Rechtfertigung von Eingriffen in das Recht auf informationelle Selbstbestimmung richtet sich allein nach den Schranken des Artikel 2 Absatz 1 Grundgesetz (vgl. BVerfG, Urteil vom 15.12.1983 – 1 BvR 209/83 u. a., juris Rn. 151). Das Zitiergebot ist auf Eingriffe in das Recht auf informationelle Selbstbestimmung nicht anwendbar (vgl. VGH Baden-Württemberg, Urteil vom 21.07.2003 – 1 S 377/02, juris Rn. 42).

Zu Nummer 4 – § 14b (Aufenthaltsanordnung und Kontaktverbot)

Mit dieser Regelung erhält der Polizeivollzugsdienst die Befugnis zur Abwehr von Gefahren in Form von terroristischen Straftaten nach § 2 Nummer 6. Den dort genannten Personen darf der Polizeivollzugsdienst demnach untersagen, sich an bestimmten Orten aufzuhalten (Aufenthaltsverbot), bestimmte Orte zu verlassen (Aufenthaltsgebot) oder Kontakt mit bestimmten Personen oder Gruppen zu haben (Kontaktverbot). Der Platzverweis nach § 14 berechtigt lediglich zu einer vorübergehenden Entfernung einer Person von einem bestimmten Ort. Die in der vorliegenden Norm geregelten Gebote und Verbote ermöglichen eine kontinuierlichere und effizientere Durchsetzung der Aufenthaltsbestimmung für die genannten Personen. Die Aufenthaltsanordnung oder das Kontaktverbot nach § 14b setzen die elektronische Aufenthaltsüberwachung nach § 33f weder voraus noch sind sie ihrerseits zwingende Voraussetzung für die Anordnung der elektronischen Aufenthaltsüberwachung nach § 33f.

Die Formulierungen zur Aufenthaltsanordnung und zum Kontaktverbot lehnen sich eng an § 56 Bundeskriminalamtgesetz 2018 und den Vorgaben des Bundesverfassungsgerichts an. Die Aufenthaltsanordnung wird in der Norm definiert als Aufenthaltsgebot oder Aufenthaltsverbot.

Absatz 1 Satz 1 regelt das Aufenthaltsgebot und das Aufenthaltsverbot. Die Befugnis zu diesem Eingriff in die freie Wahl des Aufenthaltsortes ist nur zur Verhinderung der Begehung von terroristischen Straftaten möglich. Hierdurch werden die Eingriffsbefugnisse nur auf solche Straftaten beschränkt, durch welche eine erhebliche Beeinträchtigung der hochrangigen Rechtsgüter Leib, Leben oder Freiheit drohen.

Mit Nummer 1 und Nummer 2 werden zwei verschiedene Situationen geregelt, die im Zusammenhang mit politisch motivierten Taten von Bedeutung sind. Nummer 1 erfasst insbesondere den Sachverhalt, dass im Zusammenhang mit zeitlichen Ereignissen wie z. B. Staatsbesuchen oder öffentlichen Großveranstaltungen Anhaltspunkte für eine Tatbegehung vorliegen, wobei keine konkretisierte Lage für genau diese Ereignisse vorliegen muss. Mit Nummer 2 wird dem Umstand Rechnung getragen, dass insbesondere bei Gefährdern vielfältige Anhaltspunkte für ihre Gefährlichkeit und Bereitschaft zu verheerenden Straftaten vorliegen, diese Anhaltspunkte aber noch nicht ein konkretisiertes Maß erreicht haben, die eine Zuordnung zur konkreten Begehung einer Straftat nach § 2 Nummer 6 bereits ermöglichen. Diese Unterscheidung findet sich auch in § 33a und § 33f. Mit der Verwendung der Formulierung „innerhalb absehbarer Zeit“ statt der vom Bundesverfassungsgericht gewählten Formulierung „innerhalb eines übersehbaren Zeitraums“ ist inhaltlich keine Änderung verbunden. Hiermit wird lediglich die bereits in § 2 Nummer 3 Buchstabe a) verwendete Formulierung zur besseren Nachvollziehbarkeit für die Rechtsanwenderinnen und Rechtsanwender gewählt.

Nach dem Urteil des Bundesverfassungsgerichts zu den Befugnissen des BKA-Gesetzes (Urteil vom 20.04.2016 – 1 BvR 966/09 u. a.) ist der Gesetzgeber nicht von Verfassung wegen gezwungen, Sicherheitsmaßnahmen stets nur auf die Abwehr von konkreten Gefahren zu beschränken. Allerdings bedarf es bei Maßnahmen zur Straftatenverhütung zumindest einer auf bestimmte Tatsachen und nicht allein auf allgemeine Erfahrungssätze gestützten Prognose, die auf eine konkrete Gefahr bezogen ist. Grundsätzlich gehört hierzu, dass insoweit ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist. In Bezug auf terroristische Straftaten kann der Gesetzgeber stattdessen aber auch darauf abstellen, ob

das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie in überschaubarer Zukunft terroristische Straftaten begehen wird. Denkbar sei letzteres etwa, wenn eine Person aus einem Ausbildungslager für Terroristen im Ausland in die Bundesrepublik Deutschland einreist (vgl. BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 u. a., juris Rn. 112 und 164).

Mit der Abweichungsbefugnis in Satz 2 soll entsprechend § 14 Absatz 2 Satz 3 Halbsatz 1 dem Verhältnismäßigkeitsgrundsatz Rechnung getragen werden. Denn die Anordnung darf an die Lebensführung der betroffenen Person keine unzumutbaren Anforderungen stellen. Die Wahrnehmung berechtigter Interessen darf ihr nicht unmöglich gemacht werden. So muss es der betroffenen Person grundsätzlich weiterhin möglich sein, beispielsweise einen Arzt, Rechtsanwalt, soziale Einrichtungen oder Behörden und Gerichte aufzusuchen oder sich Zugang zu öffentlichen Verkehrsmitteln zu verschaffen, sofern insoweit nicht das Kontaktverbot nach Absatz 2 greift oder andere Gründe der Gefahrenabwehr dem widersprechen.

Absatz 2 Satz 1 definiert das Kontaktverbot. Mit dem Kontaktverbot soll insbesondere vermieden werden, dass sich politisch motivierte Kriminelle untereinander verständigen, Informationen austauschen und Straftaten verabreden oder vorbereiten können. Die Ausnahmeregelung nach Absatz 2 Satz 2 entspricht derjenigen in Absatz 1 Satz 2.

In Absatz 3 wird eine Regelung getroffen, um gegenüber Personen eine Aufenthaltsanordnung auszusprechen, denen eine Ausreise ins Ausland nach den dort genannten Normen untersagt wurde. Die in den zitierten Normen geregelten Fälle betreffen Situationen, in denen die innere oder äußere Sicherheit oder sonstige erhebliche Belange der Bundesrepublik Deutschland gefährdet wurden oder eine schwere staatsgefährdende Gewalttat vorbereitet wurde. Die betroffenen Personen sollen von der Ausreise abgehalten werden, um zu verhindern, dass sie im Ausland terroristische Straftaten begehen oder sich dort in sog. Terrorcamps ausbilden lassen, um dann mit dem erworbenen Wissen terroristische Straftaten im In- oder Ausland zu begehen.

Aufgrund der Tragweite des Eingriffs in die Grundrechte des Betroffenen ist die Entscheidung über die Anordnung nach Absatz 4 Satz 1 dem Gericht vorbehalten. Bei Gefahr in Verzug, z. B. wenn entsprechende konkrete Anzeichen für eine Absetzung in das Ausland bestehen und eine Entscheidung eines Gerichts nicht unmittelbar herbeigeführt werden kann, ist eine Eilentscheidung durch die Behördenleitung angemessen, sofern das Gericht umgehend die Möglichkeit der Überprüfung dieser Maßnahme erhält. Entsprechend der bereits in § 32 Absatz 2 Satz 5 bestehenden Regelung wird die Geltung der Eilanordnung auf drei Tage begrenzt.

Zuständig ist das Amtsgericht der beantragenden Polizeidienststelle, d.h. Bremen oder Bremerhaven. Das gerichtliche Verfahren bei der Anordnung der Maßnahme richtet sich nach den Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit (FamFG). Da im Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit (FamFG) keine speziellen Regelungen zur Aufenthaltsanordnung und zu Kontaktverboten enthalten sind, gelangen die dortigen Vorschriften nur entsprechend zur Anwendung.

Der Begriff „Behördenleitung“ im Sinne des Absatzes 4 und den weiteren Nennungen dieses Gesetzes umfasst stets auch die Behördenvertretung.

Zu Nummer 5 – § 15 (Durchsetzungsgewahrsam)

Nummer 5 regelt den Gewahrsam zur Durchsetzung der Maßnahmen zur Festlegung und Bestimmung des Aufenthaltsortes. Hierdurch soll vermieden werden, dass zunächst nach § 15

Absatz 1 Satz 1 Nummer 2 geprüft werden muss, ob der Straftatbestand des § 84 Absatz 1 erfüllt ist oder nicht.

Der bloße Verstoß gegen § 14b oder § 33f ist nach Nummer 5 nicht ausreichend. Vielmehr muss die Gewahrsamnahme darauf abzielen, dass ohne ihre Anordnung die Betroffenen der Aufenthaltsanordnung oder dem Kontaktverbot nicht Folge leisten oder die elektronische Aufenthaltsüberwachung andernfalls nicht wirksam werden kann.

Im Übrigen wird eine redaktionelle Anpassung vorgenommen.

Zu Nummer 6 – § 29 Absatz 3 und 4 (Videobeobachtung und Videoaufzeichnung)

Zu Buchstabe a) – § 29 Absatz 3 (Videobeobachtung)

Absatz 3 in seiner bisherigen Fassung ermöglicht die Videoüberwachung nur an Orten, an denen vermehrt Straftaten begangen werden oder sie besonders zu erwarten sind. Damit schränkt die Norm die Befugnisse zur Gefahrenvorsorge und -abwehr auf solche Orte ein, an denen die allgemeine Kriminalitätsrate hoch ist oder örtliche Faktoren die Begehung von Straftaten besonders begünstigen. Hiernach ist eine Videoüberwachung zum Schutz besonders hochrangiger Rechtsgüter wie Leib, Leben oder Freiheit selbst dann nicht möglich, wenn Informationen darüber vorliegen, dass Tätergruppen diese Orte für die Begehung solcher Straftaten nutzen, die eine besondere Intensität und besondere Tragweite für die Betroffenen aufweisen. Ohne die Ausweitung der Videoüberwachung auf die genannten Orte würden gerade in Anbetracht der Erkenntnisse aus den zurückliegenden Monaten und Jahren die Möglichkeiten der präventiven Gefahrenabwehr im Bereich der politisch motivierten Kriminalität sowie der massiven gleichzeitigen Straftatenbegehung nicht ausreichend genutzt.

Daher werden in Absatz 3 Nummer 2 bis 4 die räumlichen Möglichkeiten zur Videoüberwachung auf besonders sensible Orte erweitert, die äußerst anfällig für Gefahren für Leib, Leben und Freiheit sind. Die hier genannten Orte sind als sog. „weiche Ziele“ potenzielle Anschlagsorte und damit besonders gefährdete Bereiche. Mit der Aufnahme dieser und zugleich Beschränkung auf diese Orte soll den Erkenntnissen aus bisherigen Straftaten in Europa und konkret Deutschland im Sinne der Gefahrenabwehr und -vorsorge Rechnung getragen werden. Auch wenn die bloße Anwesenheit der Videoüberwachung isoliert betrachtet einen terroristischen Anschlag oder die Begehung von Straftaten möglicherweise nicht verhindern kann, so stellt diese polizeiliche Maßnahme dennoch einen sehr wichtigen Baustein bei der Bekämpfung der Kriminalität dar, da Täter aufgrund der Entdeckungsgefahr vor der Begehung von Straftaten abschreckt werden können und die Polizei die Möglichkeit erhält, besser bei konkreten Gefahrensituationen in das Geschehen eingreifen zu können.

An den in Nummer 2 bis 4 genannten Orten führt die Videoüberwachung zu Eingriffen in das Recht auf informationelle Selbstbestimmung. Zumindest bei den Orten nach Nummer 2 werden aufgrund der hohen Frequentierung dieser Orte von Passanten voraussichtlich viele Personen gefilmt werden. In der Regel wird es sich hierbei um Personen handeln, von denen keine Gefahr ausgeht. Die Ausübung der Befugnisse ist daher nur unter strengen Anforderungen zulässig. Aus diesem Grund beschränkt das Gesetz die Videoüberwachung auf die vorliegenden Fälle. Soweit die öffentlich zugänglichen Räume nicht im öffentlichen Eigentum stehen, dürfen bei Einwänden von Eigentümern diese Orte nicht mittels Videoüberwachung nach Absatz 3 erfasst werden. Insoweit sind dann Vorkehrungen zu treffen, dass diese Orte nicht von der Videoüberwachung erfasst werden oder diese Bildausschnitte nicht verwendet werden.

Für die in Nummer 2 bis 4 genannten Orte ist anders als nach Nummer 1 keine konkrete Gefahrenlage in dem Sinne erforderlich, dass eine statistische Auswertung von Straftaten vorliegen muss. Es handelt sich insoweit um eine Maßnahme, die in erster Linie der Gefahrenvorsorge zuzurechnen ist. Insbesondere im Vorfeld terroristischer Straftaten sind Überwachungsmaßnahmen auch dann zulässig, wenn zwar noch kein konkretisiertes und zeitlich absehbares strafbares Geschehen oder gar eine konkrete Gefahr erkennbar ist, jedoch das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie terroristische Straftaten in überschaubarer Zukunft begehen wird. Der Staat darf bereits im Vorfeld von konkreten Gefahren Aktivitäten entfalten, um die Entstehung von Gefahren zu verhindern und um eine wirksame Bekämpfung sich ggf. erst zu einem späteren Zeitpunkt realisierender konkret drohender Gefahren zu ermöglichen (siehe BVerwG, Urteil vom 25.01.2012 – 6 C 9/11, juris Rn. 29). Dabei ist vor allem zu berücksichtigen, welche Auswirkungen bei der Begehung dieser Straftaten drohen, welchen Rang die potenziell betroffenen Rechtsgüter haben und welche Intensität der Beeinträchtigung von den Straftaten ausgehen kann.

Die mit der Videobeobachtung und -aufzeichnung für einen begrenzten Zeitraum verbundenen Eingriffe in das Grundrecht auf informationelle Selbstbestimmung (vgl. dazu u. a. VGH Baden-Württemberg, Urteil vom 21.07.2003 – 1 S 377/02, juris Rn. 34 f.) sind gerechtfertigt. Absatz 3 und Absatz 4 stellen verfassungsgemäße Schranken des Grundrechts auf informationelle Selbstbestimmung dar.

Der Einzelne muss Einschränkungen seines Rechts auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse hinnehmen. Hierzu bedarf es (nach Artikel 2 Absatz 1 Grundgesetz) einer verfassungsmäßigen gesetzlichen Grundlage. Diese muss die Voraussetzungen und den Umfang der Beschränkungen klar und für den einzelnen Bürger erkennbar hergeben, um dem rechtsstaatlichen Gebot der Normenklarheit und dem Verhältnismäßigkeitsgrundsatz zu entsprechen (auch zum vorgenannten VGH Baden-Württemberg, Urteil vom 21.07.2003 – 1 S 377/02, juris Rn. 40). § 29 Absatz 3 Satz 1 verwendet sowohl den Begriff der Bildübertragung als auch der Bildaufzeichnung. Für die Bürgerinnen und Bürger ist damit klar erkennbar, dass die Bilddaten auch vorübergehend (vgl. Absatz 4) gespeichert werden.

Die Nummer 2 bis 4 nennen Orte, die insbesondere für die Begehung politisch motivierter Straftaten von besonderer Bedeutung sind. Dies gilt für Orte nach Nummer 2 aufgrund ihrer Hochfrequentierung von Personen, nach Nummer 3 aufgrund ihrer hohen Systemrelevanz und nach Nummer 4 aufgrund der Grundrechts- bzw. Symbolbedeutung.

Nummer 2 nennt öffentlich zugängliche Orte, an denen sich gleichzeitig sehr viele Menschen aufhalten und die daher zum einen für Taten aus dem politisch motivierten Spektrum insbesondere aufgrund der dort zu erzielenden verheerenden Auswirkungen in Betracht gezogen werden, um die dortigen Menschenansammlungen zu betreffen. Zum anderen sind es aber gleichzeitig Orte, bei denen größere Menschenansammlungen zusammenkommen und die Gefahr in der Gruppe selbst entsteht und in der Gruppe wirkt. Zu den hier genannten Orten zählen beispielsweise die Bus- und Straßenbahnhaltestelle Am Brill, die Bahnhofsvorplätze des Hauptbahnhofs und des Bahnhofs Vegesack, der Marktplatz und Domshof. Hierzu zählen aber auch Orte, die nur vorübergehend als solche bestehen, wie die Weihnachtsmärkte und der Freimarkt. Nicht nur politisch motivierte Straftaten, sondern auch Straftaten, die zeitgleich und gehäuft von einer Vielzahl von Personen vorgenommen werden, haben erhebliche Auswirkungen auf die Ausübung der Freiheitsrechte der Bürgerinnen und Bürger. So zeigen die massiven, da vielfältig und gleichzeitig begangenen, sexuellen Übergriffe und Vermögensdelikte in Köln, Hamburg und Bielefeld sowie in weiteren Großstädten in der Silvesternacht vom 31.12.2015 auf den 01.01.2016 und den darauffolgenden Wochen bis heute Auswirkungen auf das Freiheits- und Sicherheitsgefühl von sehr vielen Personen in Deutschland. Ebenso führen Massenschlägereien von verfeindeten Gruppen in diesen öffentlichen Räumen, die sich mitunter sehr spontan er-

eignen, zum Verlust von Räumen der freien Entfaltung für Bürgerinnen und Bürger. Die Dynamik und das Ausmaß solcher Ereignisse gehen weit über die sog. Alltagskriminalität, die insbesondere über Nummer 1 abgedeckt wird, hinaus. Es handelt sich zudem um eine offene und keine verdeckte Maßnahme, sodass die strengeren Anforderungen für verdeckte Maßnahmen hier nicht anzulegen sind.

Die Nummer 3 und 4 sind ebenfalls in diesem Zusammenhang zu sehen. Zum einen halten sich in vielen Amtsgebäuden wie Behörden und Gerichten ebenfalls viele Menschen gleichzeitig auf, zum anderen haben die Beeinträchtigungen dieser Institutionen sowie die Beeinträchtigung von wesentlichen Infrastruktureinrichtungen wie zentrale Gas-, Strom- und/oder Wasserversorgungsanlagen erhebliche Auswirkungen für das Gemeinwesen. Die Begehung terroristischer Straftaten auf die genannten symbolischen Orte wie z. B. auf die Bürgerschaft, das Bremer Rathaus, zentrale Sakralbauten (hier: aufgrund der Eigentumsverhältnisse bei Einwänden des Eigentümers nur Videobeobachtung im Umfeld) etc. haben eine sehr intensive Auswirkung auf das Freiheitsgefühl und auf die Grundrechtsbetätigung der Bürgerinnen und Bürger. Der Anwendungsbereich von Nummer 3 und 4 wird durch die Formulierungen „wichtige“ bzw. „bedeutende“ und die Bezugnahme auf die terroristische Straftat eingeschränkt. Zu den wichtigen Versorgungsanlagen zählen insbesondere Kraftwerke, Umspannwerke, Gasspeicher und Wasserwerke. Zu den bedeutenden Amtsgebäuden zählen insbesondere das Haus der Bürgerschaft, das Rathaus, das Justizzentrum sowie zentrale Einrichtungen der Polizei. Zusätzlich müssen tatsächliche Anhaltspunkte für die Bewertung vorliegen, dass an diesen Orten mit terroristischen Straftaten zu rechnen ist. Allgemeine Erfahrungswerte reichen hierfür nicht aus. Vielmehr ist erforderlich, dass aufgrund allgemeiner Lageerkenntnisse über eine terroristische Bedrohungssituation die Gefahr eines Anschlags auf bestimmte Orte in der Freien Hansestadt Bremen hinreichend wahrscheinlich ist (vgl. VG Hannover, Urteil vom 09.06.2016 – 10 A 4629/11).

Verfassungsrechtlich ist anerkannt, dass die Polizeibehörden auch im Vorfeld einer konkreten Gefahr bereits ereignis- und verdachtsunabhängige Maßnahmen der Datenerhebung vornehmen dürfen, um Straftaten zu verhindern. Eine solche Befugnis muss jedoch im besonderen Maße dem Verhältnismäßigkeitsgrundsatz entsprechen (siehe auch zum vorgenannten VerfGH Sachsen, Urteil vom 14.05.1996 – Vf. 44-II-94, juris Rn. 230; VGH Baden-Württemberg, Urteil vom 21.07.2003 – 1 S 377/02, juris Rn. 49).

Die Videoüberwachung der genannten Orte ist ein geeignetes Instrument, um die Rechtsgüter Leib, Leben oder Freiheit zu schützen. Sie erfüllt mehrere Zwecke: Sie kann potenzielle Täter abschrecken, im Polizeieinsatz dient sie der Unterbindung von sich anbahnenden oder unmittelbar stattfindenden Straftaten gegenüber anderen Personen, durch sie werden Vorbereitungshandlungen und Ausspähversuche wahrgenommen, sie dient zur Unterstützung im Einsatzgeschehen sowie mittelbar – über die Verwertung der erlangten Erkenntnisse – im Rahmen der Strafverfolgung und bei der Berücksichtigung der erlangten Erkenntnisse bei zukünftigen präventiven Polizeieinsätzen. Die Videoüberwachung stellt einen von vielen Bausteinen der Gefahrenvorsorge und -abwehr dar und ist nicht als isoliertes Instrument einzusetzen. Eine bloße Verdrängung von Straftaten durch die Videoüberwachung ist angesichts der örtlichen Besonderheiten, die in Nummer 2 bis 4 jeweils Voraussetzung sind, nicht anzunehmen. Eigenschaften wie die des zentralen Platzes in der Innenstadt mit vielen symbolträchtigen Gebäuden und einer Vielzahl an Menschen (Marktplatz und Domshof) oder des jeweiligen zentralen Vorplatzes der Bahnhöfe für Bremen-Stadt (Hauptbahnhof) oder Bremen-Nord (Vegesack) lassen sich nicht ohne weiteres verändern.

Der Einsatz der Videoüberwachung an den genannten Orten ist auch erforderlich. Der isolierte Mehreinsatz von Polizeivollzugskräften stellt keine Alternative dar, um im gleichen Maße Straftaten zu verhindern. Die Situation im Bremer Haushalt ist äußerst angespannt. Gleiches gilt für die Personalsituation im Allgemeinen. Spielraum für Mehreinätze an den genannten Orten be-

steht nur in einem äußerst eingeschränkten Umfang. Personaleinstellungen sind nur begrenzt möglich. Die durch die Videoüberwachung erreichbare Überwachungswirkung wäre durch den alleinigen Einsatz von Polizeikräften nicht zu gewährleisten. Aufgrund der insoweit sehr viel höheren Kosten wären derartige Personalmaßnahmen auch weniger verhältnismäßig (vgl. auch zum vorgenannten VGH Baden-Württemberg, Urteil vom 21.07.2003 – 1 S 377/02, juris Rn. 53; VG Hannover, Urteil vom 14.07.2011 – 10 A 5452/10, juris Rn. 32). Zudem bietet die Videoüberwachung aufgrund der technischen Möglichkeiten (z. B. Nachtsicht, Zoom, Sicht von oben) deutlich verbesserte Möglichkeiten der Gefahrerkennung und -abwehr bei widrigen Sichtverhältnissen als der bloße Mehreinsatz von Polizeivollzugskräften. Zudem ermöglicht die Videoaufzeichnung zugleich die Dokumentation des Vorgehens von Tatverdächtigen und Tätern und damit eine bessere polizeiliche Auswertemöglichkeit sowie im Strafverfahren auch eine bessere Beweismöglichkeit.

Die isolierte Videobeobachtung ohne oder nur mit anlassbezogener Aufzeichnung in diesen öffentlichen Räumen könnte den Schutz der Rechtsgüter nicht im gleichen Maße gewährleisten. Ohne Aufzeichnung der Handlungen und Straftaten könnten diese im Nachhinein nicht oder allenfalls unter sehr erschwerten Bedingungen im Bedarfsfall ausgewertet oder verfolgt werden. Die Strafverfolgung und damit die konkret-präventive (jeweiliger Täter) und generell-präventive Gefahrenabwehr (Abschreckung anderer Täter) wären nicht möglich. Auch lägen keine Erkenntnisse zur Berücksichtigung bei der Verhinderung zukünftiger Gefahren und Straftaten vor. Gerade bei den massiven Übergriffen in der Silvesternacht 2015/2016 und den darauffolgenden Wochen hat sich namentlich die schlechte Beweislage aufgrund des nicht oder allenfalls eingeschränkt vorhandenen Bildmaterials als sehr problematisch bei der Ahndung der begangenen Straftaten erwiesen. Aufgrund der fehlenden Videoüberwachung konnten sich die Einsatzkräfte zudem kein umfangreiches Bild über die Ausmaße der Übergriffe und der Tätergruppen verschaffen, um auf dieser Grundlage gezielt den unmittelbar stattfindenden, oder im Rahmen einer Auswertung auch zukünftigen, Übergriffen zu begegnen.

Insbesondere für die Identifizierung von terroristischen Straftätern stellen Videoaufzeichnungen ein bedeutendes Instrument zur Gefahrenabwehr in Form der Analyse dar. So können sich Sachverhalte auf dem Monitor ggf. zunächst als unbedenklich oder eingeschränkt bedenklich darstellen (z. B. Ablegen eines Rucksacks), sodass eine lediglich anlassbezogene Aufzeichnung zu spät greifen würde und wichtige Informationen zur Ergreifung der Täter, der Aufklärung von Tätergruppen und -strukturen sowie zur Berücksichtigung bei vergleichbaren Handlungen fehlen würden. So konnten Täter und Tätergruppen bei terroristischen Anschlägen oftmals nur anhand des aufgezeichneten Videomaterials ermittelt und die hierdurch erlangten Erkenntnisse (z. B. Täterstrukturen, Vorgehen bei der Tatbegehung etc.) weitere Anschläge verhindert werden.

Die Ausweitung der Videoüberwachung auf die hier genannten öffentlichen Orte ist auch verhältnismäßig im engeren Sinne. Die Beeinträchtigung des Grundrechts auf informationelle Selbstbestimmung steht nicht außer Verhältnis zur Gewährleistung des Schutzes von Leib, Leben und Freiheit. Die Tragweite des Eingriffs in das Recht auf informationelle Selbstbestimmung relativiert sich insoweit als die Videoüberwachung offen erfolgt und ausschließlich das Verhalten der Betroffenen an den dort genannten Orten betrifft. Sowohl bei den in Nummer 2 genannten intensiv frequentierten Plätzen als auch bei den in Nummer 3 und 4 genannten Orten handelt es sich zudem in aller Regel um Beobachtungen, die aufgrund der kurzen Verweildauer der Personen an dem Ort nur von geringer Intensität sind. Aufgrund der offenen Kennzeichnung der Videoüberwachung in Bild und Schrift besteht die Möglichkeit, diese Bereiche zu erkennen und sich insoweit hier nicht oder nur kurz aufzuhalten. Die Freie Hansestadt Bremen greift nicht in den besonders schutzbedürftigen Bereich der Privat- oder Intimsphäre der Bürgerinnen und Bürger ein. Die von den Personen aufgrund ihres Aufenthalts an den Orten preisge-

gebenen Informationen in Form des Verhaltens können andere Personen oder die Polizeivollzugskräfte durch gleichzeitigen Aufenthalt an dem Ort ebenfalls erlangen.

Der Eingriff ist im Übrigen nur zulässig zum Schutz der sehr hochrangigen Rechtsgüter Leib, Leben und Freiheit. Die Beobachtung und Aufzeichnung (für einen begrenzten Zeitraum) kommt demnach nicht mit dem Ziel in Betracht, andere Rechtsgüter von geringerem Gewicht zu schützen. Durch die Videoüberwachung an hochfrequentierten Plätzen nach Nummer 2 werden ebenso wie an Orten, mit hoher System- (Nummer 3) oder Grundrechts- bzw. Symbolbedeutung (Nummer 4) mehr Grundrechtsträger betroffen als nach Nummer 1. Die Gefahren für die öffentliche Sicherheit, die an diesen Orten von der politisch motivierten Kriminalität aber bei Nummer 2 auch von der intensiven Massenkriminalität ausgehen, haben eine ungleich höhere Auswirkung auf das gesellschaftliche Zusammenleben als bei Orten nach Nummer 1. Es werden bei Nummer 2 bis 4 deutlich mehr Menschen geschützt als nach Nummer 1. Zudem haben massive Übergriffe innerhalb derselben Gruppe oder auf andere, verfeindete Personengruppen oder terroristische Anschläge an diesen Orten erhebliche Auswirkungen auf die Wahrnehmung der Grundrechte. Die massiven Übergriffe in der Silvesternacht 2015/2016 haben ebenso wie die Terroranschläge in Deutschland und Europa Verhaltensveränderungen zur Folge und führten und bedingen zum Teil weiterhin, dass Bürgerinnen und Bürger sich nicht gleichermaßen frei in der Öffentlichkeit bewegen, wie dies vor diesen Vorfällen der Fall gewesen ist. Die Häufigkeit der Übergriffe in größeren Personengruppen, Massenschlägereien sowie die terroristischen Anschläge in Deutschland und Europa haben gezeigt, dass sich diese Gefahren grundsätzlich jederzeit realisieren können.

Der Verhinderung und (repressive) Aufklärung von Straftaten kommt nach dem Grundgesetz eine hohe Bedeutung zu (vgl. BVerfG, Urteil vom 14.07.1999 – 2226/94 u. a., Rn. 260). Die Ausweitung auf die in Nummer 2 bis 4 genannten räumlichen Bereiche trägt – auch in Anbetracht der häufigeren Betroffenheit von Passanten – diesem Umstand durch die Einschränkung zum Schutz der hochrangigen Rechtsgüter angemessen Rechnung. Die Videoüberwachung nach Nummer 1 richtet sich nach der Häufigkeit der Straftaten und damit stärker nach der Einzelfallbetroffenheit. Demgegenüber orientiert sich der Schutz in Nummer 2 bis 4 stärker an den Auswirkungen auf die öffentliche Gemeinschaft, das Zusammenleben der Bürginnen und Bürger in der freiheitlich demokratischen Grundordnung, der Grundrechtsbetätigung im öffentlichen Raum und den Auswirkungen der massiven Beeinträchtigungen auf eine Vielzahl von Menschen.

Aufgrund der intensiven Vorbereitungszeit für die Einrichtung der Videoüberwachung in Form von Konzepten, technischen und baulichen Prüfungen sowie den Anschaffungs- und Herrichtungskosten, sollte eine solche Maßnahme eine angemessene Mindestlaufzeit aufweisen können. Die bisherige Formulierung, wonach in „regelmäßigen“ Zeitabständen die Voraussetzungen der Einrichtung zu überprüfen ist, war insoweit zu offen formuliert. Die Präzisierung gibt der Bürgerschaft die Möglichkeit, die Maßnahmen regelmäßig innerhalb von 2 Jahren zu überprüfen und schafft zugleich Planungssicherheit für die Einrichtung und Aufrechterhaltung einer solchen Maßnahme. Das Zustimmungserfordernis des Senators für Inneres gewährleistet die Vorabkontrolle vor der Einrichtung und Betriebsaufnahme der Videoüberwachung. Die Bürgerinnen und Bürger erhalten vor Ort durch Beschilderung einen Hinweis auf die Vornahme der Videoüberwachung sowie die Kontaktdaten der verantwortlichen Stelle.

Zu Buchstabe b) – § 29 Absatz 4 (Videoaufzeichnung)

Der bisherige einzige Satz wird in drei Sätze unterteilt, um die Anforderungen präzise zu beschreiben.

Die Löschfristen für Aufzeichnungen nach Absatz 1 und 2 sowie Absatz 3 Nummer 1 bleiben unberührt.

Die Aufzeichnung stellt gegenüber der Bildübertragung einen intensiveren Grundrechtseingriff dar. Dieser Eingriff ist an den Orten nach Nummer 2 bis 4 gerechtfertigt. Zunächst sind die Auswirkungen auf die freiheitlich demokratische Grundordnung und damit das Zusammenleben aller Bürgerinnen und Bürger durch die oben genannten Gefahren ungleich größer als bei der nach Nummer 1 erforderlichen Straftatbegehung. Die von der Bilderübertragung ausgehenden Einwirkungen auf das Recht auf informationelle Selbstbestimmung würden bei Nummer 2 bis 4 ohne die Aufzeichnung weitestgehend leer laufen. Denn gerade die Aufzeichnung des Bildmaterials ermöglicht oftmals erst die Auswertung und somit die Identifizierung von auffälligem Verhalten und auffälligen Personen oder gar von Straftätern und leistet daher einen erheblichen Beitrag zur Gefahrenabwehr. Eine weitergehende Belastung der Betroffenen würde erst im Falle der Auswertung der Aufzeichnungen und damit im Regelfall nicht zum Tragen kommen (siehe auch VGH Baden-Württemberg, Urteil vom 21.07.2003 – 1 S 377/02, juris Rn. 63). Den Zugriff auf die Videoüberwachungsdaten erhält zudem weiterhin nur ein ausgewählter Kreis an Polizeivollzugskräften, wie Videobeobachter, Beamte des Lagezentrums und ggf. Systemadministratoren. Der im Einzelfall möglichen Beeinträchtigung von weiteren Grundrechten (etwa die Erfassung einer Versammlung im Sinne des Artikels 8 Absatz 1 Grundgesetz) ist durch entsprechende Vorgaben zur Handhabung in einer Dienstanweisung Rechnung zu tragen. Hinsichtlich des Umfangs und der Intensität der Auswirkungen auf die Bürgerinnen und Bürger ist diese Maßnahme daher angemessen.

Die bisher in Absatz 4 geregelte Speicherfrist von 48 Stunden wird den aktuellen und zukünftigen Bedarfen der polizeilichen Praxis gerade in Anbetracht der zunehmenden Gefahr terroristischer Anschläge nicht gerecht. Für die Speicherung von Videobeobachtungen nach Absatz 3 Nummer 2 bis 4 sind längere Speicherfristen erforderlich. Die Innenministerkonferenz hat mehrfach bekräftigt, dass das Instrument der Videoüberwachung einen wichtigen Beitrag für eine erfolgreiche Terrorismusbekämpfung darstellt, und sich dafür ausgesprochen, das Instrument stärker zu nutzen. Die polizeilichen Erkenntnisse und Erfahrungen haben gezeigt, dass die Speicherungsfristen von 48 Stunden im Bereich der politisch motivierten Kriminalität und bei massiven Übergriffen nicht ausreichen, um der Gefahrenabwehr, insbesondere zur Verhinderung geplanter terroristischer Straftaten oder Aufklärung von diesen, Rechnung zu tragen. Hinweisen zu Terroreinheiten von ausländischen Sicherheitsbehörden kann oftmals nur mit zeitlichen Verzögerungen (z. B. aufgrund eines Übersetzungs- und Abstimmungsbedarfes etc.) polizeilich nachgegangen werden. Sofern im Nachgang von Hinweisen oder Erkenntnissen das Videomaterial ausgewertet werden soll, um die Begehung einer solch gravierenden Straftat zu verhindern oder Täter bzw. Tätergruppen zu identifizieren, würde eine Speicherfrist von nur 48 Stunden, wie es die Regelung zu Abs. 3 Nr. 1 vorsieht, etwaige Ermittlungsansätze von Vornherein unterbinden. Bei massiven Übergriffen wie in der Silvesternacht 2015/2016 kann die Identifizierung eines etwaigen Tatanteils sich erst aufgrund weiterer Hinweise und Auswertungen ergeben, für die entsprechend Bearbeitungszeit vorzusehen ist. In Anbetracht dieser Umstände und der gebotenen Begrenzung der Speicherfrist auf das erforderliche Maß ist zur Erfüllung des Zwecks eine Speicherfrist in diesen Fällen auf maximal 30 Kalendertage angemessen.

Zu Nummer 7 bis 12 und 14 – §§ 33a bis 33e, 33g (Telekommunikationsmaßnahmen)

In den zurückliegenden Jahren hat sich die Telekommunikation rasant weiterentwickelt. An fast jedem Ort können Telefonate geführt, E-Mails, SMS und sonstige Text- oder Bildnachrichten versendet und empfangen werden. Sogar Videotelefonie und Videonachrichten können mit modernen Mobilfunkgeräten (Handys, Tabletgeräte, Smartwatches etc.) aufgenommen und versendet werden. Die Geräte sind dazu in der Lage, sämtliche Informationen aus dem Internet aufzurufen oder einzuspeisen. Inzwischen bedarf es hierfür sogar nicht einmal mehr Handys,

sondern es können auch sog. Smartwatches, also Armbanduhren mit elektronischem Display und Internetanschluss Bestandteile der vorgenannten Kommunikation übernehmen. Mit diesen positiven Möglichkeiten der Vernetzung erweitern sich allerdings auch die Möglichkeiten Krimineller. Unabhängig vom jeweiligen Standort können Kriminelle weltweit kommunizieren, sich austauschen und Taten organisieren. Sie erhalten hierdurch die Möglichkeit, sich sehr viel schneller und intensiver unabhängig von festen Standorten auszutauschen und Taten vorzubereiten und zu verabreden. Insbesondere im Bereich der Organisierten Kriminalität und der politisch motivierten Kriminalität werden die Möglichkeiten der Telekommunikation ausgeschöpft. Straftaten mit gravierenden Auswirkungen für die einzelnen Bürgerinnen und Bürger, für das gesellschaftliche Zusammenleben sowie für den Bestand der Länder und des Bundes können hierdurch unter erleichterten Voraussetzungen durchgeführt werden.

Zur Aufdeckung von Anschlagsplanungen und zur Vermeidung ihrer Umsetzung ist eine Verifizierung von Gefährdungshinweisen maßgeblich vom Zugang zu Informationen aus dem Kommunikationsaufkommen der Kriminellen abhängig. Dies gilt gerade für die Suche nach Zusammenhängen in staaten- und länderübergreifenden Netzwerken, aber auch für die Aufdeckung von Befehls- und Nachrichtenketten wie auch für Wege der Radikalisierung und der informellen Anbindung von sog. Rekruten. Dabei spielt namentlich das Internet eine wichtige Funktion bei der Vorbereitung und Begehung von politisch motivierten Straftaten und der Rekrutierung weiterer Straftäter. Denn hierdurch wird unmittelbar eine sehr große Gruppe ungefiltert und mit wenig technischem Aufwand (anders als z. B. Presse, Funk und Fernsehen) angesprochen und im Rahmen einer Organisationsstruktur gelenkt. Diese Medien sind insofern das Werkzeug der Rekrutierung, der Mobilisierung und der informellen Vernetzung. Islamistische Terroristen oder rechtsextreme Gruppen und Organisationen verbreiten ihre Propaganda über das Internet und tauschen sich in Foren oder Chats über die Begehung von Straftaten aus.

Ein weiteres Anwendungsfeld der präventiven Telekommunikationsüberwachung ist die Schutzgelderpressung durch Täter der Organisierten Kriminalität. Die Opfer dieser Taten verweigern in der Regel die Angaben aus Furcht vor Repressalien der Täter. Dadurch kann aber oftmals kein ausreichender Anfangsverdacht begründet werden, der aber für die Telekommunikationsüberwachung nach der Strafprozessordnung erforderlich wäre. Durch die präventive Telekommunikationsüberwachung können entsprechende Angaben ermittelt, präventiv eingegriffen und später vor Gericht gegen die Täter verwendet werden.

Von Bedeutung sind die Befugnisse auch im Bereich der Kinderpornographie. Die in diesem Bereich organisierten Täter gehen sehr abgeschottet vor und tauschen sich vor allem über das Internet aus. Auch in der organisierten Drogenkriminalität spielt die Telekommunikationsüberwachung eine wichtige Rolle. Beispielsweise werden die Verkäufe und die Übergaben über Mobilfunkgeräte verabredet. Dadurch können sich die Straftaten von den Gefahrenorten verlagern und im gesamten Landesgebiet begangen werden. Auch bei der sog. Amokgefahr sind die Befugnisse, hier konkret die Standortermittlung und die Telekommunikationsüberwachung, von besonderer Bedeutung, wenn die Polizei z. B. die Aussage von anderen Personen erreicht, eine Person habe die Absicht mitgeteilt, Amok zu laufen und der aktuelle Aufenthaltsort dieser Person zunächst ermittelt werden muss.

Die Maßnahmen dienen auch zum Schutz derjenigen Personen, deren Mobilfunkgeräte geortet werden. So können demenzkranke, hilfsbedürftige, entführte oder vermisste Personen mittels Standortermittlung ihrer Mobilfunkgeräte schneller aufgefunden und in die Obhut von Vertrauenspersonen oder Ärzten übergeben werden. Ohne die Standortermittlung können diese Personen nicht oder allenfalls über sehr umfangreiche und lange währende Sucheinsätze ermittelt werden. Diese Zeit steht oftmals in diesen Fällen nicht zur Verfügung. Kündigt z. B. eine suizidgefährdete Person ihre Absicht an, sich das Leben nehmen zu wollen, kann mittels Standortermittlung der Aufenthaltsort dieser Person unmittelbar ermittelt und ihr umgehend Hilfe zugeführt

werden, bevor sie eine unumkehrbare Handlung vornimmt.

Um eine effektive Gefahrenabwehr auch weiterhin sicherzustellen, wird der Polizeivollzugsdienst der Freien Hansestadt Bremen in die Lage versetzt, die Telekommunikationsüberwachung (TKÜ) auch präventiv, d.h. vor Begehung einer Straftat durchführen zu können. Aufgrund der Tragweite dieses Eingriffs in die Rechte Einzelner, sind hohe Anforderungen an die berechtigten Interessen zum Schutz der Grundrechte zu erfüllen.

Telekommunikationsüberwachung bezeichnet das Abhören und/oder Aufzeichnen von Telefongesprächen oder Nachrichten aller Art. Die Telekommunikationsüberwachung hat die Inhaltsdaten zum Gegenstand.

Die Telekommunikationsüberwachung zielt nicht auf die Auskunft über Verkehrsdaten und Bestandsdaten. Verkehrsdaten sind diejenigen technischen Informationen, die bei der Nutzung eines Telekommunikationsdienstes beim jeweiligen Telekommunikationsunternehmen anfallen und von diesem erhoben oder verarbeitet werden. Hierzu zählen u. a. der in Anspruch genommene Telekommunikationsdienst (Telefonie, Internetnutzung, Videotelefonie etc.), die Nummer der beteiligten Anschlüsse, Standortdaten, Beginn und Ende der jeweiligen Verbindung sowie weitere Daten, die den Rahmen der Telekommunikationsverbindung bilden. Unter Bestandsdaten werden diejenigen Angaben verstanden, die der Telekommunikationsanbieter dauerhaft vom Kunden speichert. Hierzu zählen beispielsweise die Angaben des Kunden bei Vertragsschluss wie z. B. Name und Adresse sowie die IP-Adresse (Identifizierung des Geräts im Internet) etc.

Bei der Quellen-Telekommunikationsüberwachung wird die Telekommunikationsüberwachung direkt am Gerät des Betroffenen (der Quelle) durchgeführt, bevor ein Telekommunikationsdiensteanbieter die dort anfallenden Inhalte weiterleitet. Anlass dieser Maßnahme sind Verschlüsselungen, die bereits auf dem Gerät durchgeführt werden und durch welche die erst beim Telekommunikationsdienstanbieter abzugreifenden verschlüsselten Inhalte für die präventive Gefahrenabwehr weitestgehend nicht zu verwenden sind. Mittels der Quellen-Telekommunikationsüberwachung kann die Polizei vor der Verschlüsselung die Inhalte abrufen. Die Begriffe „Quellen-Telekommunikationsüberwachung“ und „Onlinedurchsuchung“ werden gelegentlich synonym verwendet. Gemeinsam haben beide Maßnahmen, dass hier direkt auf einen Computer, Mobilfunkgerät o. ä. zugegriffen wird und dies unter Umgehung von technischen Schutzmaßnahmen geschieht. Allerdings haben beide Maßnahmen unterschiedliche Tragweiten: Zwar wird bei der Onlinedurchsuchung ebenfalls direkt auf das Gerät des Betroffenen zugegriffen, allerdings mit einer anderen Zielrichtung. Bei der Telekommunikationsüberwachung und der Quellen-Telekommunikationsüberwachung dürfen nur zukünftige Inhalte erfasst werden (laufende Telekommunikation). Demgegenüber dürfen bei der sog. Onlinedurchsuchung sämtliche Inhalte – auch die in der Vergangenheit liegenden, in Form von vorhandenen Dateien – in Gänze abgerufen und verwertet werden. Analog zur Hausdurchsuchung gibt es insofern mit Ausnahme von Informationen, die dem Kernbereich persönlicher Lebensgestaltung zuzurechnen sind, grundsätzlich keinen Bereich, welcher von der Onlinedurchsuchung ausgeschlossen wäre. Die Onlinedurchsuchung ist nicht Gegenstand des vorliegenden Gesetzesentwurfs.

Bei der Standortfeststellung wird mittels Abruf verschiedener Funkzellen (festgelegte Bereiche zwischen mehreren Mobilfunkantennen) ermittelt, an welchem Standort sich ein Mobilfunkgerät und damit in aller Regel die Person gerade befindet.

Neben dem Abrufen von Inhalten beim Telekommunikationsdiensteanbieter (Telekommunikationsüberwachung), direkt am Gerät (Quellen-Telekommunikationsüberwachung), dem Abruf von Verbindungsinformationen (Verkehrsdatenauskunft) sowie von Rahmendaten über den Telekommunikationsteilnehmer (Bestandsdaten) kommt u. a. auch die Ortung des Mobilfunkgeräts

(Standortabfrage) und die Unterbrechung von Telekommunikationsverbindungen in Betracht. Mit der Unterbrechung von Telekommunikationsverbindungen soll vermieden werden, dass Täter eine Straftat initiieren, z. B. indem sie ein Startsignal an andere Personen geben oder mittels Fernzündung Sprengsätze auslösen.

Die Telekommunikationsüberwachung und die Befugnisse im Zusammenhang mit Telekommunikationsgeräten sind in §§ 100a ff. der Strafprozessordnung (StPO) für die Strafverfolgung geregelt. In der polizeilichen Praxis haben sich diese Befugnisse bewährt. Allerdings ist zwingende Voraussetzung für ihre Anwendbarkeit, dass ein qualifizierter Anfangsverdacht im Sinne des § 170 Strafprozessordnung vorliegt. Es muss daher bereits ein Strafverfahren gegen einen Tatverdächtigen eingeleitet worden sein, damit die Überwachungsmaßnahmen der Telekommunikation nach der Strafprozessordnung durchgeführt werden können. Die Ermittlungen müssten insofern überhaupt erst tatsächliche Erkenntnisse über Zusammenhänge, Methoden und Kontakte erbracht haben, um eine Telekommunikationsüberwachung aus Gründen der Strafverfolgung vornehmen zu können. Damit ist aber ein frühzeitiges Erschließen der Täterstrukturen, der grundsätzlichen Organisation und Abläufe etc. zum Zwecke der Gefahrenabwehr erschwert, wenn nicht gar verhindert.

Das bisherige Nichtenthalten der Befugnisse im Bremischen Polizeigesetz führt zu dem unbefriedigenden Ergebnis, dass mit der Telekommunikationsüberwachung zwar Straftaten effektiv verfolgt, nicht aber bereits vor ihrer Umsetzung effektiv verhindert werden können. Darüber hinaus stellt sich die Lage widersprüchlich dar, weil unter bestimmten Voraussetzungen zwar das mit weitergehenden Eingriffen in die Grundrechte verbundene Abhören in Wohnungen zu Zwecken der Gefahrenabwehr zulässig wäre, aber die weniger grundrechtsbelastende Überwachung des Telekommunikationsverkehrs nicht möglich wäre.

Aufgrund der Auswirkungen auf die geschützten Grundrechte unterliegen die Maßnahmen entsprechenden Voraussetzungen. Eine dieser Voraussetzungen ist die Abwehr einer bevorstehenden Gefahr für die hochrangigen Rechtsgüter Leib, Leben oder Freiheit oder Bestand oder Sicherheit des Bundes/des Landes oder seiner Einrichtungen. Nur vor diesem Hintergrund ist der Eingriff in die Grundrechte der Betroffenen (insbesondere in das nach Artikel 10 Grundgesetz geschützte Fernmeldegeheimnis) gerechtfertigt (vgl. BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09, juris Rn. 109).

Der Landesgesetzgeber besitzt die Gesetzgebungskompetenz für diese Regelungen. Die ausschließliche Gesetzgebungszuständigkeit des Bundes nach Artikel 73 Absatz 1 Nummer 7 Grundgesetz auf dem Gebiet des Postwesens und der Telekommunikation steht nicht im Widerspruch zur Regelungskompetenz der Freien Hansestadt Bremen für die genannten Maßnahmen. Denn nach der Rechtsprechung des Bundesverfassungsgerichts umfasst das Post- und Telekommunikationswesen nur die technische Seite des Übermittlungsvorgangs im Kommunikationsbereich und nicht die Regelungen über die übermittelten Inhalte.

Da die Eingriffe in die Grundrechte zunächst verdeckt vorgenommen werden, haben die Betroffenen selbst keine Möglichkeit, das Handeln des Polizeivollzugsdienstes zu überprüfen. Der Parlamentarische Kontrollausschuss kontrolliert daher auch die Durchführung dieser Maßnahmen. Die Parlamentarische Kontrolle, wie sie in § 36 geregelt ist, bedarf infolge der Aufnahme dieser Befugnisse keiner Anpassung. § 36 Absatz 1 umfasst mit seiner Bezugnahme auf „§§ 33 bis 35“ bereits zutreffender Weise die neu einzufügenden Befugnisse in §§ 33a bis 33d (und § 33f). Damit trägt der Gesetzgeber den verfassungsrechtlichen Anforderungen an eine regelmäßige Kontrolle außerhalb der befugten Stellen Rechnung (vgl. BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09, juris Rn. 143).

Zu Nummer 7 – § 33a (Telekommunikationsüberwachung und Eingriff in TK)

Absatz 1 regelt die Telekommunikationsüberwachung. Der Begriff Telekommunikation ist in § 3 Nummer 22 Telekommunikationsgesetz definiert als technischer Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen, wobei letztgenannte technische Einrichtungen oder Systeme sind, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können (§ 3 Nummer 23 Telekommunikationsgesetz).

Für die polizeiliche Gefahrenabwehr sind drei Anwendungsbereiche 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 automatisch auch Verkehrsdaten an die Polizei übermittelt, da z. B. Dauer der Übermittlung, das Telekommunikationsmittel etc. mitgeteilt. Zum anderen können auch Mailboxen überprüft werden, in deren Datenspeicher innerhalb des Telekommunikationsnetzes Nachrichten 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 auch der Standort des Benutzers übermittelt. Dies gilt sowohl für den Fall, dass mit dem Mobilfunktelefon ein Gespräch geführt wird, als auch für den Fall, dass sich das Mobilfunktelefon lediglich im Stand-by-Modus befindet.

In Absatz 1 Satz 1 Nummer 1 bis 3 werden die Voraussetzungen geregelt, unter denen der Einsatz dieses Mittels zulässig ist. Der Adressatenkreis orientiert sich an der Regelung in § 32 Absatz 1 Satz 1 Nummer 1 und 2. Die Überwachungsmaßnahmen dürfen nach Nummer 1 gegenüber Störern im Sinne der §§ 5 und 6 zur Abwehr einer gegenwärtigen Gefahr für die abschließend aufgezählten hochrangigen Rechtsgüter durchgeführt werden. Durch die Beschränkung auf hochrangige Rechtsgüter und durch die höhere Gefahrenschwelle wird dem Umstand Rechnung getragen, dass es sich um einen weitgehenden Grundrechtseingriff handelt.

Nummer 2 eröffnet den Anwendungsbereich auch für die Gruppe der potenziellen terroristischen Attentäter und der Gefährder. Die Regelung trägt der besonderen Tragweite der terroristischen Straftaten Rechnung. Zur Unterscheidung nach Nummer 1 und Nummer 2 und der Begründung siehe oben die Begründung zu Nummer 4. Das Bundesverfassungsgericht hat in seinem Urteil zum Bundeskriminalamtgesetz die Ermöglichung der Telekommunikationsüberwachung im Vorfeld einer konkreten Gefahr (vgl. Nummer 1) nicht beanstandet. Damit diese Vorverlagerung nicht zu einer zu intensiven Ausweitung führt, werden entsprechende Anforderungen an die Erkenntnisse gestellt (vgl. BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09, juris Rn. 112, 213).

Die Maßnahme kann darüber hinaus nach Nummer 3 zur vorbeugenden Bekämpfung von besonders schwerwiegenden Straften zur Anwendung gelangen. Nummer 3 erweitert hierzu den Personenkreis auch auf solche Personen, die zwar nicht selbst unmittelbar an der jeweiligen Tatvorbereitung/-begehung beteiligt sind, aber als Boten zwischengeschaltet sind oder ihre Telekommunikationsanlagen für die Tatbegehung zur Verfügung stellen. Die Erfassung auch dieser Personen ist verfassungsrechtlich zulässig (BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 u. a., juris Rn. 116.).

Nach Satz 2 sind Datenerhebungen nur zulässig, wenn die polizeiliche Aufgabenerfüllung auf andere Weise aussichtslos oder wesentlich erschwert wäre. Hierdurch wird dem Verhältnismäßigkeitsgrundsatz Rechnung getragen, wonach zunächst andere gleich effektive Mittel angewandt werden müssen, bevor dieses Mittel genutzt wird.

Absatz 2 Satz 1 trägt dem Umstand Rechnung, dass mit der Telekommunikationsüberwachung in die Privatsphäre der Betroffenen eingegriffen wird. Die verfassungsrechtliche Rechtsprechung benennt die Inhalte von Gesprächen, die höchstpersönlich dem Kernbereich der privaten Lebensgestaltung zuzurechnen sind, als so gewichtig, dass eine gezielte Überwachung derartiger Gesprächsinhalte unzulässig ist (vgl. BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 u. a., juris Rn. 125). Hinsichtlich des Kernbereichsschutzes im Zusammenhang mit der Telekommunikationsüberwachung hat das Bundesverfassungsgericht ausgeführt, dass der Schutz beim Fernmeldegeheimnis anders ausgestaltet ist, als der beim Grundrecht auf Unverletzlichkeit der Wohnung. Denn die Bürger seien zur höchstpersönlichen Kommunikation nicht in gleicher Weise auf die Telekommunikation angewiesen wie auf eine Wohnung. Allerdings fordere der Grundsatz der Menschenwürde auch im Gewährleistungsbereich des Artikels 10 Grundgesetz Vorkehrungen zum Schutz individueller Entfaltung im Kernbereich privater Lebensgestaltung. Bestehen also im konkreten Fall tatsächliche Anhaltspunkte für die Annahme, dass eine Telekommunikationsüberwachung Inhalte erfasst, die zum Kernbereich zählen, so ist diese nicht zu rechtfertigen und muss unterbleiben. Da aber bei der Anordnung der Telekommunikationsüberwachung oder bei ihrer Durchführung nicht sicher vorhersehbar ist, welchen Inhalt die Gespräche oder Nachrichten haben werden, ist das Risiko nicht auszuschließen, dass die Abhörmaßnahme Kommunikation aus dem Kernbereich erfasst. Dieses Risiko ist allenfalls bei einem besonders hohen Rang des gefährdeten Rechtsguts und einer durch konkrete Anhaltspunkte gekennzeichneten Lage, die auf einen unmittelbaren Bezug zur zukünftigen Begehung einer Straftat schließen lässt, hinzunehmen. Für den Fall, dass es ausnahmsweise zur Erhebung kernbereichsrelevanter Inhalte gekommen ist, müssen daher Vorkehrungen getroffen werden, die sicherstellten, dass diese nicht gespeichert und verwertet werden dürfen, sondern unverzüglich gelöscht werden (BVerfG, Urteil vom 27.07.2005 – 1 BvR 668/04, juris Rn. 162 ff.). Dieses Vorgehen setzt voraus, dass die Zuordnung zum Kernbereich der privaten Lebensgestaltung bereits vorgenommen werden kann. Ist dies nicht der Fall und soll ein Gericht als externe Stelle über die Verwertbarkeit entscheiden, ist eine Speicherung bis zur Entscheidung des Gerichts verfassungsrechtlich zulässig (vgl. BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 u. a., juris Rn. 218 ff.). Der hier ebenfalls angesprochene Schutz von Berufsgeheimnisträgern zählt gleichermaßen zu den verfassungsrechtlich aufgestellten Grenzen. Der von §§ 53 und 53a Strafprozessordnung ausgehende Schutz ist für die Durchführung fairer Gerichtsverfahren von solcher Bedeutung, dass dieser Schutz nicht durch die Telekommunikationsüberwachung umgangen werden darf.

An diesen Grundsätzen orientiert sich die vorgeschlagene Regelung in Absatz 2 Satz 1 bis 4. Aufgrund der normierten hohen Voraussetzungen – der Abwehr einer Leib- oder Lebensgefahr bzw. einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder der Begehung von terroristischen Straftaten, die gemeinhin dieselben Rechtsgüter betreffen, welche zudem auch bei der Umgehung der Maßnahmen zu Nummer 1 und 2 durch Boten oder andere Kommunikationsmittel betroffen sind – und der Bedeutsamkeit dieser Rechtsgüter ergibt die Abwägung mit den bei Maßnahmen nach Absatz 1 Satz 1 betroffenen Grundrechten, dass das Risiko einer Kernbereichsverletzung vertretbar ist. Anders als bei der Wohnraumüberwachung ist es bei der Telekommunikationsüberwachung aufgrund der Vielfalt der in Betracht kommenden Gesprächspartner und der anderen Kommunikationssituation in der Regel nicht möglich, im Vorwege zu erkennen, ob es sich um Gespräche handelt, die einen unmittelbaren Bezug zum Kernbereich der privaten Lebensgestaltung haben. Wenn aber erkennbar wird, dass tatsächlich kernbereichsrelevante Gespräche geführt werden, so gelten die für die Wohnraumüberwachung entwickelten Grundsätze entsprechend. Darüber hinaus erfolgt der Kernbereichsschutz und Schutz der Berufsgeheimnisträger auf der zweiten Stufe über die Kennzeichnungs- und Löschungsgebote sowie über das Verwertungsverbot.

In Absatz 2 Satz 1 wird die Situation geregelt, dass die Überschreitung dieser Grenzen bereits abzusehen ist. Satz 2 bis 5 regeln hingegen den Fall, dass sich die Betroffenheit des Kernbe-

reichs oder ein Gespräch/ein Schriftwechsel mit einem Berufsgeheimnisträger nicht vorab ankündigt und insoweit diese Betroffenheit ohne zeitlichen Vorlauf eintreten kann. In diesen Fällen ist die Überwachung grundsätzlich zu unterbrechen. Um bei Zweifeln nicht automatisch die potenziell für die Gefahrenabwehr sehr wichtigen Informationen nicht mehr verwenden zu können, kann nach Satz 3 eine automatische Erfassung – ohne Sinneswahrnehmung durch die Polizeivollzugskräfte – erfolgen und ist dieses Material umgehend dem zuständigen Gericht als insoweit Dritten zwecks Freigabe oder Vernichtung vorzulegen. Diese Regelung trägt dem Umstand Rechnung, dass der Grundrechtseingriff im Falle der Verwendung seitens der Polizei ohne externe Prüfung zu weitgehend wäre, wenn der Kernbereichsschutz oder der Schutz der Berufsgeheimnisträger betroffen wäre, wohingegen eine automatische Nichtverwertung bei Zweifeln die Erhebung relevanter Daten und damit die Gefahrenabwehr ggf. zu frühzeitig verhindern würde. Die Regelung stellt somit einen angemessenen Ausgleich zwischen dem Aufklärungsinteresse zum Schutz der genannten hochrangigen Rechtsgüter einerseits und dem berechtigten Grundrechtsschutz andererseits dar (vgl. BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 u. a., juris Rn. 129, 224). Wenn die intensive Grundrechtsbetroffenheit hingegen nicht mehr anzunehmen ist, besteht auch kein Grund mehr, auf die Befugnis zu verzichten, sodass diese nach Satz 5 wieder aufgenommen werden kann.

Eine Rechtsgrundlage für die Verbindungsunterbrechung bzw. -verhinderung wird in Absatz 3 geschaffen. Mit dieser Maßnahme sollen Telekommunikationsverbindungen der in Absatz 1 Satz 1 Nummer 1 bis 3 genannten Störer oder potentiellen Straftäter unterbrochen oder künftige Verbindungen von oder zu den Genannten verhindert werden. Terroristische Sprengstoffanschläge wurden auch durch Zündmechanismen ausgelöst, die auf ein Signal eines Mobilfunkgeräts reagiert haben. Zudem kann potentiellen Straftätern die Planung und Koordination ihres Vorhabens erheblich erschwert werden, wenn die Telekommunikation unterbrochen wird. So kann beispielsweise die Mitteilung des Startsignals zur Tatbegehung mittels Unterbrechung verhindert werden und so die unmittelbare Tatbegehung verhindert werden. Die Polizei kann so die notwendige Zeit gewinnen, um anderweitige Maßnahmen zu ergreifen, mittels derer die Gefahr endgültig beseitigt werden kann. Satz 2 ermöglicht eine solche Maßnahme auch gegenüber Dritten. Wegen des erheblichen Grundrechtseingriffs ist dies jedoch nur zulässig zur Abwehr von Gefahren für Rechtsgüter von überragender Bedeutung. Insoweit räumt Satz 2 nun auch die Befugnis ein, bei Geisellagen die Telekommunikation über Telekommunikationsgeräte der Geiseln mit Mittätern außerhalb des Tatorts zu verhindern.

Absatz 4 regelt die Mitwirkungspflichten derjenigen, die geschäftsmäßig Telekommunikationsdienste anbieten, erbringen oder daran mitwirken (Diensteanbieter). Für die Telekommunikationsüberwachung und -aufzeichnung ergeben sich diese Pflichten durch den Verweis auf das Telekommunikationsgesetz. Dort ist detailliert geregelt, auf welche Weise die Anbieter verpflichtet sind, die Polizei zu unterstützen. Die Mitwirkungspflicht erstreckt sich auch auf solche Diensteanbieter, deren Firmensitze außerhalb der Freien Hansestadt Bremen liegen, sofern sie ihre Dienste auch in der Freien Hansestadt Bremen anbieten.

Zu Nummer 8 – § 33b (Quellen-Telekommunikationsüberwachung)

Der oben beschriebene Einsatz des Internets durch Kriminelle für Gefahren für wichtige Schutzgüter der öffentlichen Sicherheit, z. B. durch die Verbreitung rechtsextremer oder islamistischer Propaganda, die Androhung von Terroranschlägen und die Nutzung des Internets durch die Organisierte Kriminalität werden dadurch vergrößert, dass vermehrt Kommunikationsvorgänge im Internet oder über das Mobilfunkgerät unter Verwendung von kryptologischen Verfahren abgewickelt werden. Immer mehr Telefongespräche werden nicht mehr auf herkömmlichem Weg, sondern über das Internet (Voice-over-IP) oder als Videotelefonie verschlüsselt geführt. Das bedeutet, dass Inhalte bereits auf dem jeweiligen Computer oder Mobilfunkgerät verschlüsselt werden können und die Inhalte verschlüsselt über den Diensteanbieter an andere

Kommunikationsteilnehmer übermittelt werden. Einige Kommunikationsprogramme wie z. B. WhatsApp haben die sog. Ende-zu-Ende-Verschlüsselung inzwischen standardmäßig aktiviert, sodass Nutzer dieser Software ohne Aufwand ihre Telekommunikation verschlüsselt übersenden. Die Telekommunikationsüberwachung nach § 33a ermöglicht in diesen Fällen keine effektive Gefahrenabwehr, da die Polizei dann nur Zugriff auf verschlüsselte Daten erhält. Eine Analyse der übermittelten Inhalte und ggf. ein sofortiges Eingreifen wäre auf dieser Informationsgrundlage nicht möglich.

Der Polizeivollzugsdienst steht – ebenso wie andere Sicherheitsbehörden oder die Strafverfolgungsbehörden – vor dem Problem, dass sich diese Form der Telekommunikation nicht beim Telefondiensteanbieter überwachen lässt, sondern nur unmittelbar bei den Kommunikationsteilnehmern an der Quelle, d.h. am unmittelbaren Gerät. Vor diesem Hintergrund hat sich hierfür der Begriff der sog. Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) herausgebildet. Für diese Form der Telekommunikationsüberwachung ist es grundsätzlich erforderlich, das Mobilfunkgerät oder Computersystem des Kommunikationsteilnehmers verdeckt mit einer speziellen Überwachungssoftware zu versehen, die anschließend die Gespräche/Nachrichten unverschlüsselt an den Polizeivollzugsdienst übermittelt. Diese Methode kommt nur dann in Betracht, wenn die Inhalte der Telekommunikation nur auf diesem Weg erlangt werden können.

Das Bundesverfassungsgericht hat in seiner Entscheidung zum Bundeskriminalamtgesetz die sog. Quellen-Telekommunikationsüberwachung für verfassungsgemäß erklärt, soweit durch rechtliche und technische Maßnahmen sichergestellt ist, dass nur die laufende Telekommunikation erhoben wird. Sowohl im Bundeskriminalamtgesetz 2018 als auch in den Polizeigesetzen der Länder Bayern, Hamburg, Hessen, Rheinland-Pfalz und Thüringen ist diese präventive Befugnis bereits enthalten.

Die Quellen-Telekommunikationsüberwachung ist nach Absatz 1 nur unter denselben strengen materiellen Voraussetzungen zulässig, die auch für Maßnahmen nach § 33a Absatz 1 gelten. Zusätzlich müssen die in § 33b genannten weiteren Anforderungen erfüllt sein.

Absatz 1 schafft eine Rechtsgrundlage für den heimlichen, technischen Eingriff in ein informationstechnisches System zum Zweck der Telekommunikationsüberwachung. Artikel 10 Grundgesetz ist alleiniger grundrechtlicher Maßstab für die Beurteilung einer solchen Ermächtigung, wenn sich die Überwachung ausschließlich auf Daten aus einem laufenden Kommunikationsvorgang beschränkt und dies durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt ist (BVerfG, Urteil vom 27.02.2008 – 1 BvR 370/07 u. a., juris Rn. 190). Aus diesem Grund erklärt Absatz 1 Nummer 1 den Eingriff in ein informationstechnisches System zur Durchführung der Maßnahme nur dann für zulässig, wenn sichergestellt ist, dass ausschließlich laufende Telekommunikation erfasst wird.

Absatz 1 Nummer 2 stellt als weitere Voraussetzung eine besondere Ausgestaltung des Verhältnismäßigkeitsgrundsatzes dar und nennt mit der Gewährleistung der Aufzeichnung von Telekommunikation in unverschlüsselter Form den Hauptanwendungsfall der Maßnahme.

Absatz 2 Satz 1 Nummer 1 bestimmt zunächst, dass beim Einsatz des technischen Mittels sicherzustellen ist, dass an dem informationstechnischen System (IT-System; Computer oder Mobilfunkgerät) nur solche Veränderungen vorgenommen werden, die für die Datenerhebung unbedingt erforderlich sind. Vor nicht unbedingt erforderlichen Veränderungen zu schützen sind nicht nur die von dem Nutzer des IT-Systems angelegten Anwenderdateien, sondern auch die für die Funktion des IT-Systems erforderlichen Systemdateien. Auch Beeinträchtigungen der Systemleistung sind auf das technisch Unvermeidbare zu begrenzen. Hierdurch wird dem Grundsatz der Erforderlichkeit Rechnung getragen, wonach nur solche Mittel zum Einsatz ge-

langen und Befugnisse nur in dem Maß genutzt werden, wie dies unbedingt notwendig ist, um das geeignete Ziel zu erreichen.

Nach Absatz 2 Satz 1 Nummer 2 sind bei Beendigung der Maßnahme alle an dem infiltrierten System vorgenommenen Veränderungen rückgängig zu machen, soweit dies technisch möglich ist. Insbesondere ist die auf dem IT-System installierte Überwachungssoftware vollständig zu löschen und sind Veränderungen an den bei der Installation der Überwachungssoftware vorgefundenen Systemdateien rückgängig zu machen. Die Einschränkung, soweit dies technisch möglich ist, geht auf den Erforderlichkeitsgrundsatz zurück. Da eine dauerhafte Veränderung im System nach Beendigung der Maßnahme für diese nicht mehr aufrechterhalten werden muss, wäre ihre Aufrechterhaltung nicht mehr verhältnismäßig. Allerdings kann aufgrund von technischen Begebenheiten auf dem betroffenen IT-System, die z. B. unabhängig von der eingesetzten Software ein dauerhaftes Löschen unterbinden, eine vollständige Wiederherstellung aller Systemdateien gegebenenfalls nicht mehr erfolgen. Dass nicht im Vornherein in Gänze ausgeschlossen werden kann, dass es zu bleibenden Veränderungen im System kommt, diese aber grundsätzlich soweit wie möglich rückgängig zu machen sind, wurde vom Bundesverfassungsgericht nicht beanstandet und hat es die Verhältnismäßigkeit bejaht (vgl. BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 u. a., juris Rn. 215).

Absatz 2 Satz 2 verpflichtet den Polizeivollzugsdienst dazu, die eingesetzten technischen Mittel vor unbefugter Nutzung zu schützen. Hierdurch soll vermieden werden, dass die Einflussnahme auf das IT-System für den Betroffenen Nachteile mit sich bringt, die er nicht zu verantworten und hinzunehmen hat. Satz 3 trägt entsprechend § 33a Absatz 2 dem Umstand Rechnung, dass durch die Überwachungsmaßnahme in den Kernbereich privater Lebensgestaltung eingegriffen werden könnte.

Absatz 3 dient dem effektiven Rechtsschutz des Betroffenen. Insbesondere ist damit sichergestellt, dass der Nachweis erbracht werden kann, dass die Daten tatsächlich vom betroffenen IT-System stammen und auf dem Weg der Erhebung nicht verändert wurden. Flüchtige Veränderungen im Sinne von Satz 1 Nummer 2 sind solche, die im Arbeitsspeicher einschließlich der Auslagerungsdatei gespeichert werden.

Satz 2 normiert eine strenge Zweckbindung der Protokolldaten. Die Daten dürfen nur verwendet werden, um einer dazu befugten Behörde, einem dazu befugten Gericht oder dem Betroffenen im Rahmen seines Auskunftsanspruchs die Prüfung der rechtmäßigen Durchführung der Maßnahme zu ermöglichen. Satz 2 führt kein neuartiges Prüfungsrecht des Betroffenen ein, sondern beschränkt die Verwendung der Protokolldaten auf die Erfüllung des allgemeinen datenschutzrechtlichen Auskunftsanspruchs des Betroffenen.

Satz 3 regelt die Aufbewahrung und Löschung der Protokolldaten.

Aufgrund der Tragweite des Eingriffs beschränkt Absatz 4 die Zielrichtung des Eingriffs ausschließlich auf die für die Gefahr verantwortlichen Personen. Da nicht ausgeschlossen werden kann, dass es zu unvermeidbarer Betroffenheit anderer Personen kommt und hierdurch nicht die Maßnahme automatisch beendet werden muss, ist die unvermeidbare Betroffenheit aus Verhältnismäßigkeitsgründen verfassungsrechtlich akzeptiert (siehe BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09, juris Rn. 115).

Zu Nummer 9 – § 33c (Verkehrsdatenerhebung und Standortermittlung)

In § 33c wird die Verkehrsdatenabfrage geregelt. Sie bezieht sich in erster Linie auf bereits erfolgte Gespräche. Es wird damit bei einer Maßnahme nach § 33c keine aktuell bestehende Telekommunikationsverbindung erfasst. Vielmehr können die Ermittler in Erfahrung bringen, wel-

che Telekommunikationsverbindungen von einem bestimmten Anschluss hergestellt wurden. Gleiches gilt auch für versandte E-Mails oder andere Nachrichten. 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.

Die Regelungen in § 33c ermöglichen allerdings auch die Gefahrenabwehr bei Personen, von denen gegenüber anderen Personen keine Gefahr ausgeht, deren Rechtsgüter Leib, Leben und Freiheit aber selbst gefährdet sind (siehe Absatz 3 Nummer 2). Diese Norm zielt ausschließlich auf den Schutz der dort genannten Personen ab.

Eine besondere Form der Verkehrsdatenabfrage ist in Absatz 2 geregelt. Es handelt sich um den sog. Zielsuchlauf oder die sog. Umkehrsuche. Der Zielsuchlauf hat nicht die Verbindungen zum Gegenstand, welche von dem überprüften Anschluss aufgebaut wurden, sondern sucht umgekehrt diejenigen Anschlüsse, welche von sich aus eine Verbindung zu dem überprüften Anschluss aufgebaut haben. Hierdurch werden Kommunikationsnetze erfasst, die andernfalls unerkannt blieben. Die Erkenntnisse über die Netzstrukturen sind aber gerade bei der Bekämpfung der politisch motivierten Kriminalität und der Organisierten Kriminalität von immenser Bedeutung für die Gefahrenabwehr.

Die Regelung in Absatz 3 ermöglicht den Einsatz von sog. IMSI-Catchern für polizeilich-präventive Zwecke. Diese Geräte können Geräte- und Kartennummern sowie den Standort von Mobilfunkgeräten identifizieren. Die Erfahrungen aus der Polizeipraxis zeigen die Notwendigkeit der Identifizierung (Nummer 1) und Standortbestimmung (Nummer 2) von Mobilfunkgeräten zur Vorbereitung von Überwachungsmaßnahmen nach § 33a Absatz 1 sowie zur Abwehr unmittelbar bevorstehender Gefahren für Leib, Leben oder Freiheit.

Die Notwendigkeit der Identifizierung von Gerätenummer und Kennung eines Mobilfunkgeräts (Nummer 1) ergibt sich aus der Tatsache, dass im Bereich der politisch motivierten Kriminalität und der Organisierten Kriminalität zunehmend Mobilfunkgeräte benutzt werden, deren Herkunft nicht bekannt ist (sog. Burner oder Burner Handys), sodass auch die Rufnummer nicht zu ermitteln ist. Für die Anordnung einer Überwachungsmaßnahme nach § 33a Absatz 1 ist aber die Rufnummer oder eine andere Kennung des Telekommunikationsanschlusses zwingend erforderlich, sodass eine Abhörmaßnahme nach § 33a Absatz 1 in diesen Fällen nicht in Betracht käme. Daher wird zur Abwehr einer unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit bzw. zur Verhinderung von besonders schwerwiegenden Straftaten die Identifizierung der Gerätenummer zur Vorbereitung einer Maßnahme nach § 33a Absatz 1 benötigt.

Hieran zeigt sich die strikt am rechtsstaatlichen Verhältnismäßigkeitsprinzip orientierte Eingriffsgrundlage, die wesentlich restriktiver ist als bei Abhörmaßnahmen gemäß § 33a Absatz 1. Die Rechtsgüterabwägung zwischen den Grundrechten der Betroffenen (Störer und Nichtstörer) einerseits und dem öffentlichen Interesse (Schutz von Leben und Gesundheit nach Artikel 2 Absatz 2 Grundgesetz) andererseits ergibt einen Vorrang für die Durchführung der schwerwiegenden Maßnahme im öffentlichen Interesse.

Die Maßnahmen nach Absatz 3 Nummer 2 dürfen nur zur Abwehr einer unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit erfolgen.

Der Polizeivollzugsdienst hat die verfassungsrechtliche Schutzpflicht für das Leben und die Gesundheit der Bürgerinnen und Bürger aus Artikel 2 Absatz 2 Grundgesetz wahrzunehmen. Diese wichtigen Rechtsgüter überwiegen die nur vorübergehend und punktuell 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 z. B. Suizidgefährdete Personen von ihrer Tat abzuhalten. Gleiches gilt für die Ortung vermisster oder 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 Person und die unverzügliche Einleitung von Rettungsmaßnahmen ermöglichen.

Absatz 4 enthält strenge Vorgaben und Einschränkungen der Maßnahme aus Gründen der Verhältnismäßigkeit. Die Erfassung von personenbezogenen Daten Dritter darf nur erfolgen, wenn dies unvermeidbar ist. Zudem sind diese Daten umgehend nach Beendigung der Maßnahme zu löschen. Damit wird dem Datenschutz von unbeteiligten Personen Rechnung getragen und die Einschränkung auf ein Minimalmaß reduziert.

Absatz 5 regelt die Übermittlung der in Absatz 6 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 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 Gründen besonderer Sachnähe als auch aus einem besonderen Pflichtenverhältnis heraus, welches sie – wie den §§ 111 ff. TKG zu entnehmen ist – gegenüber den Sicherheitsbehörden zur Bereitstellung von Daten verpflichtet. Absatz 5 Satz 3 enthält eine ausdrückliche Entschädigungsregelung für die Diensteanbieter. Die Legaldefinition des Begriffs der Verkehrsdaten in Absatz 6 orientiert sich an § 96 Telekommunikationsgesetz. Im Hinblick auf weitere zu erwartende technische Entwicklungen wird auf eine abschließende Aufzählung verzichtet.

Zu Nummer 10 – § 33d (Bestandsdatenerhebung)

Absatz 1 räumt dem Polizeivollzugsdienst die Möglichkeit ein, von den Diensteanbietern unter engen Voraussetzungen Auskunft über Bestandsdaten von Betroffenen zu erhalten. Diese Daten beinhalten u. a. den Namen und die Anschrift des Anschlussinhabers, ihm zugeteilte Rufnummern etc.

Das Bundesverfassungsgericht hat die Erhebung von Bestandsdaten auf der Grundlage der allgemeinen fachrechtlichen Eingriffsermächtigung nicht beanstandet. Allerdings hat es festgehalten, dass hinsichtlich der Eingriffsschwelle sicherzustellen ist, dass – bezogen auf die Gefahrenabwehr – eine Auskunft nur aufgrund einer konkreten Gefahr auf einzelfallbezogener Tatsachenbasis vorgenommen werden darf (BVerfG, Urteil vom 02.03.2010 – 1 BvR 256/08, juris Rn. 261).

Absatz 1 trägt der Rechtsprechung des Bundesverfassungsgerichts Rechnung, die verlangt, dass es für den Abruf der nach den §§ 95 und 111 TKG gespeicherten Daten im manuellen Auskunftsverfahren grundsätzlich einer qualifizierten Rechtsgrundlage bedarf, die selbst eine Auskunftspflicht der Telekommunikationsunternehmen normenklar begründet (BVerfG, Beschluss vom 24.01.2012 – 1 BvR 1299/05, juris Rn. 168 ff.). Dieses Erfordernis gilt auch für Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird, und für zu bestimmten Zeitpunkten zugewiesene Internetprotokoll-Adressen bzw. IP-Adressen (siehe Absatz 1 Satz 2, Absatz 2).

Zwar hat das Bundesverfassungsgericht sich im oben genannten Beschluss nur zu den Regelungen des Telekommunikationsgesetzes geäußert. Aus Klarstellungsgründen soll an dieser Stelle aber auch der Abruf von Bestandsdaten nach dem Telemediengesetz in einer spezifi-

schen Rechtsgrundlage erfasst werden. Wie weiter oben bereits beschrieben, ist es heutzutage fast schon zufällig, ob die Telekommunikation noch nach dem Telekommunikationsgesetz oder nach dem Telemediengesetz erfasst wird, da inzwischen viele Telekommunikationsverbindungen über Kanäle des Internetprotokolls bzw. mittels Voice-over-IP-Technik geführt werden.

§ 14 Absatz 2 des Telemediengesetzes legt vergleichbar § 113 Absatz 1 Satz 1 TKG fest, in welchen Fällen die Diensteanbieter zur Übermittlung der betreffenden Daten berechtigt sind.

Mit § 33d Absatz 1 wird die Auskunft über Bestandsdaten, Auskunftsersuchen, die auf Zugangssicherungscodes, wie Passwörter, PIN oder PUK abzielen sowie die Identifizierung dynamischer IP-Adressen ausdrücklich geregelt. Absatz 1 Satz 1 verpflichtet die Diensteanbieter auf Verlangen Auskunft über Bestandsdaten zu erteilen. Der Begriff der Bestandsdaten wird in Absatz 5 definiert. Die Definition deckt sich durch die Bezugnahme auf § 95 TKG mit § 3 Nummer 3 TKG – erweitert um die Daten nach § 111 TKG. Daten nach § 95 TKG sind insoweit Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden. Bestimmte Daten sind aber auch dann herauszugeben, wenn ihre Speicherung nicht für betriebliche Zwecke erforderlich sein sollte. § 111 TKG führt diese auf. Dazu gehören beispielsweise die Rufnummer und andere Anschlusskennungen, der Name und die Anschrift des Anschlussinhabers. Zum anderen besteht aber auch eine Herausgabepflicht für Bestandsdaten im Sinne des § 14 Absatz 1 des Telemediengesetzes. Nach der Rechtsprechung des Bundesverfassungsgerichts ist bei gefahrenabwehrrechtlichen Auskünften erforderlich, aber auch ausreichend, dass diese zur Abwehr einer konkreten Gefahr für die öffentliche Sicherheit benötigt werden (BVerfG, Beschluss vom 24.01.2012 – 1 BvR 1299/05, juris Rn. 177).

Auskunftsersuchen zur Gefahrenabwehr, die auf Zugangssicherungscodes wie Passwörter, PIN oder PUK abzielen, werden in Absatz 1 Satz 2 geregelt. Für solche Daten darf die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung dieser Daten vorliegen. Die Regelung orientiert sich ebenfalls an den Vorgaben des Bundesverfassungsgerichts (BVerfG, Beschluss vom 24.01.2012 – 1 BvR 1299/05, juris Rn. 183 ff.). Die Erhebung von Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen geschützt wird, ist demnach nur zulässig, wenn eine Vorschrift der Polizei die Nutzung der durch die Auskunft erlangten Daten im konkreten Fall erlaubt. Wird beispielsweise eine PIN benötigt, um die auf einem sichergestellten Mobilfunkgerät abgelegten Daten auszulesen, so müssen für die Mitteilung der Zugangssicherungscodes seitens des Diensteanbieters die Voraussetzungen des § 23 vorliegen.

Absatz 2 sieht vor, dass die Auskunft nach Absatz 1 auch anhand einer zu bestimmten Zeitpunkten zugewiesenen Internetprotokoll-Adresse sowie weiterer zur Individualisierung erforderlicher technischer Daten verlangt werden darf. Durch die Bezugnahme auf Absatz 1 gelten wiederum dessen Eingriffsschwellen. Der zweite Halbsatz soll eine individuelle Zuordnung insbesondere auch dann ermöglichen, wenn eine Internet-Protokolladresse mehrfach an verschiedene Nutzer vergeben wurde.

Absatz 3 regelt die Pflichten und die entsprechende Entschädigung der Diensteanbieter.

Zu Nummer 11 – § 33e (Anordnung und Ausführung von TK-Maßnahmen)

§ 33e regelt die verfahrensrechtlichen und datenschutzrechtlichen Vorgaben für Maßnahmen nach §§ 33a bis 33d.

Die Maßnahmen nach § 33a bis § 33c stehen danach wegen der hohen Bedeutung des Fernmeldegeheimnisses unter einem richterlichen Anordnungsvorbehalt. Nur in Ausnahmefällen,

nämlich bei Gefahr im Verzug, darf die Maßnahme – mit Ausnahme der Anordnung der Quellen-Telekommunikationsüberwachung nach § 33b – durch die Behördenleitung angeordnet werden. Der Eingriff in die informationstechnischen Systeme wird in der verfassungsrechtlichen Rechtsprechung als so weitgehend betrachtet, dass hier (§ 33b) keine Abweichung vom Richtervorbehalt bei Gefahr in Verzug in Betracht kommt (vgl. BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09, juris Rn. 216).

Im Falle der Anordnung bei Gefahr im Verzug ohne Beteiligung des Gerichts muss innerhalb von spätestens drei Tagen eine Bestätigung des Gerichts eingeholt werden. Die Maßnahmen sind zu beenden, wenn ihre Voraussetzungen nicht mehr vorliegen. Diese Klarstellung ist aus verfassungsrechtlichen Gründen geboten. Das anordnende Gericht erhält nach Beendigung der Maßnahmen, die es angeordnet hat, entsprechend Kenntnis von den Ermittlungsergebnissen (vgl. BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09, juris Rn. 265 a. E.). Auf dieser Grundlage kann das Gericht seine Entscheidungen besser begründen und bei der Entscheidung über zukünftige Anordnungen diese Erkenntnisse berücksichtigen.

Zuständig ist das Amtsgericht der beantragenden Polizeidienststelle, d.h. Bremen oder Bremerhaven. Das gerichtliche Verfahren bei der Anordnung der Maßnahme richtet sich nach den Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit (FamFG). Zwar wird mit der „entsprechenden Geltung“ bereits eine analoge Anwendung des FamFG angeordnet, mit der das Gericht den besonderen Erfordernissen des Rechts der Gefahrenabwehr gerecht werden soll. Für den Fall der vorherigen Anhörung erfolgt jedoch der besondere Hinweis, dass diese unterbleibt, wenn eine solche den Zweck der Maßnahme gefährden würde. Wird die Maßnahme nicht binnen drei Tagen richterlich bestätigt, so sind die erlangten Daten sofort zu löschen.

Absatz 2 enthält eine Abweichung von dem vorgenannten Grundsatz des Richtervorbehalts im Falle des § 33c Absatz 3 Nummer 2. Damit diese Maßnahme nicht dem Richtervorbehalt unterliegt, muss sie sich ausschließlich auf die Ermittlung des Aufenthaltsortes der genannten hilfsbedürftigen Personen beziehen. Die Maßnahme darf nicht bloßer Nebenzweck sein oder die Anforderungen des § 33e Absatz 1 Satz 1 umgehen. Aufgrund dieser Voraussetzungen ist gewährleistet, dass dieser Grundrechtseingriff ohne richterliche Überprüfung ausschließlich zum Wohle der genannten hilfsbedürftigen Personen vorgenommen wird. In diesen Fällen würde die Prüfung der Maßnahme durch ein Gericht einen zeitlichen Aufwand bedeuten, der dem Erfolg der Maßnahme, der Abwehr von unumkehrbaren Schäden für die gesuchten Personen, zuwiderlaufen würde. Die mitunter schwierige Frage, ob bereits Gefahr im Verzug nach Absatz 1 Satz 2 vorliegt oder nicht, könnte im Einsatzfall Zeitverlust bedeuten, der ausschließlich zu Lasten der Person geht, zu deren Gunsten die Maßnahme durchgeführt werden soll. Aus diesem Grund wird dieser Fall explizit in Absatz 2 geregelt. Durch den Vorbehalt der Behördenleitung bzw. entsprechend befugter Personen nach § 30 ist sichergestellt, dass die Maßnahme gleichwohl einer engen Kontrolle unterliegt. In Anbetracht der Abwägung zwischen der Intensität der Gefahren, die insbesondere bei den genannten Personen vorliegen, namentlich erhebliche oder gar unumkehrbare Schäden für die hochrangigen Rechtsgüter Leib und Leben, und den Verfahrensvorgaben einerseits und dem durch die Standortermittlung erfolgenden Grundrechtseingriff zu Lasten und zugleich zu Gunsten der betroffenen Person andererseits ist der sehr enge Verzicht auf den Richtervorbehalt angemessen.

Nach Absatz 3 ist die Anordnung in schriftlicher Form zu erlassen und hat in der Regel die genaue Bezeichnung des Betroffenen und der Maßnahme einschließlich ihres Umfangs und der Dauer sowie die Angabe der Rufnummer oder einer anderen Kennung zu enthalten. Durch die Alternative, statt der Rufnummer auch die Kennung des Telekommunikationsanschlusses, des Endgeräts oder des informationstechnischen Systems ausreichen zu lassen, wird die sog. IMEI-gestützte-Überwachung eines Mobilfunkgeräts ermöglicht. Mobilfunkendgeräte übertragen ne-

ben der sog. IMSI-Nummer auch stets die sog. IMEI-Nummer. Die IMSI-Nummer ist einer Mobilfunkgerätkarte (SIM-Karte) zugeordnet, während die IMEI-Nummer einem Gerät zugeordnet ist. Wechselt der Nutzer des Gerätes seine Mobilfunkkarte, verändert sich hierdurch zwar die Rufnummer und die IMSI-Nummer, aber nicht die IMEI-Nummer. Etliche Störer verfügen teilweise über zahlreiche verschiedene Mobilfunkgerätkarten, die sie abwechselnd zumeist in demselben Mobilfunkgerät einsetzen. Dadurch ändert sich die zu überwachende Kennung des Mobilanschlusses, und müsste ohne diese Regelung stets zunächst die neue Kennung des Anschlusses ermittelt werden, um anschließend eine auch auf diese Kennung bezogene gerichtliche Entscheidung herbeiführen zu können. Ohne diese Regelung könnten Störer daher alleine durch den Wechsel ihrer Mobilfunkkarte eine Unterbrechung der Überwachung herbeiführen. Diese Regelung ermöglicht daher die möglichst unterbrechungsfreie Überwachung der Telekommunikation des Störers über das von ihm eingesetzte Gerät.

In den Fällen, in denen die Zweckerreichung sonst aussichtslos oder erheblich erschwert wäre, kann z. B. 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 maximal drei Monate mit einer Verlängerungsmöglichkeit von jeweils bis zu drei weiteren Monaten unter der Bedingung, dass die Voraussetzungen weiterhin vorliegen. Aus der verfassungsrechtlichen Rechtsprechung folgt, dass die maximal zulässige Dauer der Anordnung für den Eingriff in das informationstechnische System nach § 33b Absatz 1 im Einzelfall kürzer ausfallen kann und entsprechend zu bemessen ist (siehe BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09, juris Rn. 216 a. E.).

Hinsichtlich der Maßnahme der Telekommunikationsunterbrechung und -verhinderung wird wegen der erheblichen Eingriffsintensität eine deutlich geringere Frist von zwei Wochen bzw. zwei Tagen festgesetzt.

Absatz 4 bis 6 regeln besondere verfahrenssichernde Maßnahmen. Es handelt sich um datenschutzrechtliche Kennzeichnungs-, Zweckänderungs-, Unterrichtungs- und Löschungsregelungen.

In Absatz 4 werden das Kennzeichnungsgebot und die Verwendungsbeschränkungen geregelt. Die Kennzeichnung der aus der Telekommunikationsüberwachung 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, deren Verwendung zum Schutz anderer hochrangiger Rechtsgüter erforderlich ist.

Präzisiert wurden auch die Unterrichtungsvorschriften in Absatz 5. Diese Regelungen dienen insbesondere der verbesserten Wahrnehmung effektiven Rechtsschutzes. Die Zurückstellung der Benachrichtigung bedarf jeweils nach sechs Monaten der richterlichen Zustimmung (§ 33e Absatz 5 Satz 2 in Verbindung mit § 33 Absatz 5 Satz 2). In den besonders in § 33e Absatz 5 Satz 2 in Verbindung mit § 33 Absatz 5 Satz 5 aufgeführten Fallkonstellationen kann mit richterlicher Zustimmung eine Benachrichtigung auch auf Dauer unterbleiben.

Die besonderen Löschungsregelungen in Absatz 6 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, deren Verwendung zum Schutz anderer hochrangiger Rechtsgüter erforderlich ist.

Zu Nummer 12 – § 33f (elektronische Aufenthaltsüberwachung)

Die Maßnahme stellt einen weiteren Baustein zur Bekämpfung der politisch motivierten Kriminalität und insbesondere des internationalen Terrorismus‘ dar. Als Ergänzung zu den bestehenden Überwachungsmöglichkeiten der Sicherheitsbehörden kann es geboten sein, dass der Polizeivollzugsdienst präventiv die elektronische Aufenthaltsüberwachung (EAÜ) anordnet, wenn entsprechende Anhaltspunkte vorliegen, welche die Annahme einer Begehung einer terroristischen Straftat im Sinne des § 2 Nummer 6 durch die betroffene Person begründen.

Mit dieser Maßnahme soll der Aufenthaltsort von Personen, von denen die Gefahr der Begehung einer terroristischen Straftat im Sinne von § 2 Nummer 6 ausgeht, ständig überwacht werden und auf diese Weise die Begehung terroristischer Straftaten verhindert werden. Die ständige Aufenthaltsüberwachung steigert das Risiko auf Seiten der Störer, bei der Vorbereitung oder Begehung von Straftaten entdeckt zu werden, und kann auf diese Weise zur Straftatenverhütung beitragen. Darüber hinaus ermöglicht die ständige Aufenthaltsüberwachung das schnelle Eingreifen der Polizei zur Straftatenverhütung.

Die elektronische Aufenthaltsüberwachung wird bereits im repressiven Bereich als Mittel der Führungsaufsicht zur Überwachung aus dem Straf- oder Maßregelvollzug entlassener Personen eingesetzt (siehe § 68b Absatz 1 Satz 1 Nummer 12 Strafgesetzbuch in Verbindung mit § 463a Strafprozessordnung). Im präventiven Bereich wird die Überwachung nach § 56a Aufenthaltsgesetz und § 56 Bundeskriminalamtgesetz 2018 ebenfalls eingesetzt. Die hier aufgenommene Befugnis steht selbstständig neben den genannten Befugnissen.

Die Überwachungsmaßnahme setzt sich technisch aus einem Sender und einer sog. Hauseinheit zusammen. Mittels eines Bandes wird der Sender am Arm oder Bein des Störers befestigt. Da die Befestigung am Fußgelenk weniger auffällig ist und die Betroffenen hierdurch weniger in ihrem Alltag betroffen sind als im Falle der sichtbaren Befestigung am Arm o. ä., wird der Sender in aller Regel am Fußgelenk befestigt. Hierdurch wurde der Begriff „elektronische Fußfessel“ geprägt, der in Diskussionen synonym zur elektronischen Aufenthaltsüberwachung verwendet wird. Manipulationen an der Befestigung oder dem Sender lösen eine Alarmmeldung aus. Die Positionsbestimmung erfolgt grundsätzlich mittels GPS-Signal. Die Hauseinheit dient als Basisstation und wird fest am Wohnsitz des Probanden installiert. Sobald sich der Sender im Bereich der Hauseinheit befindet, wird dies registriert und die Übermittlung von Positionsdaten innerhalb des Wohnraums eingestellt.

Die Norm orientiert sich stark an den präventiv-rechtlichen Vorschriften des § 56a Aufenthaltsgesetz und § 56 Bundeskriminalamtgesetz 2018 sowie den einschlägigen gesetzgeberischen Handlungsempfehlungen einer Bund-Länder-Arbeitsgruppe.

Gerade unter Verhältnismäßigkeitsgesichtspunkten ist die elektronische Aufenthaltsüberwachung als offene Maßnahme weniger einschneidend als eine ständige Observation, bei der nicht nur der Aufenthaltsort, sondern auch die Handlungen und Gesprächspartner der betroffenen Person überwacht werden und dadurch ein sehr viel umfangreicheres Persönlichkeitsbild

entstehen kann als bei der Übertragung der bloßen Standortdaten. Insoweit stellt die elektronische Aufenthaltsüberwachung ein milderes Mittel dar.

Zur Unterscheidung nach Absatz 1 Nummer 1 und Nummer 2 und der Begründung siehe oben die Begründung zu Nummer 4. Wie bereits ausgeführt wurde, ist der Gesetzgeber nicht verpflichtet, Sicherheitsmaßnahmen stets nur auf die Abwehr von konkreten Gefahren zu beschränken (vgl. BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 u. a.). Zur Begrenzung des Anwendungsbereichs müssen „bestimmte Tatsachen“ vorliegen bzw. muss die „konkrete Wahrscheinlichkeit begründet“ sein. Durch diese Formulierungen wird deutlich, dass allgemeine Erfahrungen und Lageerkenntnisse nicht ausreichen und insoweit vielmehr anhand personenbezogener Informationen eine entsprechende Bewertung vorliegen muss, die eine Begehung einer terroristischen Straftat innerhalb absehbarer Zeit erwarten lässt. Eine konkrete Gefahr ist demnach für die Anordnung dieser Maßnahme gerade nicht erforderlich. Im Falle einer konkreten Gefahr wären anderweitige Befugnisse des Polizeivollzugsdienstes vorrangig zu prüfen.

Absatz 2 greift die Rechtsgedanken des § 14b Absatz 3 auf.

Absatz 3 folgt im Wesentlichen dem Vorbild des § 463a Strafprozessordnung, der die Befugnisse der Aufsichtsstellen bei der Führungsaufsicht sowie die von diesen einzuhaltenden datenschutzrechtlichen Vorgaben regelt. Die Verarbeitung umfasst dabei grundsätzlich alle Aufenthaltsdaten einschließlich der Daten über eine Beeinträchtigung der Erhebung. Dieser umfassende Ansatz ist erforderlich, um sämtliche in Satz 9 Nummer 1 bis 5 vorgesehenen Verwendungszwecke erfüllen und die mit der Überwachung angestrebten Wirkungen erreichen zu können. Der Befugnis zur Erhebung von Daten über etwaige Beeinträchtigungen bei der Datenerhebung bedarf es nicht nur für eine effektive Gefahrenabwehr und Strafverfolgung, sondern auch, um davon unabhängige Funktionsbeeinträchtigungen erkennen zu können, die z. B. eine Reparatur der vom Betroffenen mitgeführten Geräte erfordern.

Die Datenerhebung und -speicherung hat automatisiert zu erfolgen (Absatz 3 Satz 1). Dies soll – zusammen mit der Vorgabe in Satz 11 – die Einhaltung der unterschiedlichen Verwendungszwecke sichern und gewährleisten, dass die zuständige Behörde grundsätzlich nur die Daten zur Kenntnis nehmen kann, die für die Erfüllung dieser Zwecke erforderlich sind.

Soweit es technisch möglich ist, ist sicherzustellen, dass innerhalb der Wohnung der betroffenen Person keine über den Umstand ihrer Anwesenheit hinausgehenden Aufenthaltsdaten erhoben werden. Dem Schutz des Kernbereichs privater Lebensführung wurde durch die Regelungen in Absatz 3 Satz 2 bis 7 Rechnung getragen. Damit wird dem Betroffenen ermöglicht, einen innersten Rückzugsraum zu haben, in dem er vom Staat nicht behelligt wird. Eine genaue Ortung innerhalb der Wohnung ist damit untersagt. Die Regelung in Satz 2 bis 7 verfolgt dabei einen abgestuften Ansatz: Soweit dies technisch möglich ist, dürfen die genannten Aufenthaltsdaten gar nicht erst erhoben werden. Sollte technisch ein Ausschluss dieser Daten nicht umgesetzt werden können, darf jedenfalls eine Verwertung dieser Daten nicht erfolgen. Sie sind unverzüglich zu löschen, sobald eine Kenntnisnahme erfolgt ist, wobei die Tatsache ihrer Kenntnisnahme und Löschung gemäß Satz 6 zu protokollieren ist. Die Regelung gewährleistet, dass die elektronische Aufenthaltsüberwachung nicht zu einem unzulässigen Eingriff in den Kernbereich privater Lebensführung führt.

Satz 9 regelt die einzelnen Verwendungszwecke für die übermittelten Daten. Nach Nummer 4 dürfen die Daten auch zur Abwehr einer erheblichen gegenwärtigen Gefahr für das Leben, die körperliche Unversehrtheit oder die persönliche Freiheit einer Person verwendet werden. Könnten die Daten nicht für diese Zwecke genutzt werden, würde ein erheblicher Vertrauensverlust in die Funktionsfähigkeit der Polizei und damit der staatlichen Institutionen insgesamt drohen, wenn trotz einer elektronischen Aufenthaltsüberwachung die entsprechenden Daten nicht zur

Verfolgung oder Verhinderung erheblicher Straftaten, insbesondere von schweren Gewaltstraftaten, genutzt werden dürften. Die wirksame Aufklärung gerade schwerer Straftaten ist ein wesentlicher Auftrag des rechtsstaatlichen Gemeinwesens (vgl. BVerfG, Urteil vom 03.03.2004 – 1 BvR 2378/98, juris Rn. 200), ebenso wie die Abwehr erheblicher Gefahren für hochrangige Rechtsgüter. Nach Nummer 5 dürfen die Daten auch zur Aufrechterhaltung der Funktionsfähigkeit der technischen Mittel verwendet werden. Die Regelung gestattet die Verwendung von Daten, die auf eine nicht vom Betroffenen zu vertretende Funktionsbeeinträchtigung hinweisen, um diese – z. B. durch Austausch der vom Betroffenen mitgeführten Geräte – beseitigen zu können. Denn die Überprüfung der Funktionsfähigkeit der eingesetzten Geräte ist Grundvoraussetzung für eine Nutzung der Daten nach Nummer 1 bis 4.

Die Verwendung der Daten für die vorgenannten Zwecke stellt einen Eingriff in das Recht auf informationelle Selbstbestimmung dar, der verhältnismäßig ist. Sie verfolgt den Zweck, Gefahren für hochrangige Rechtsgüter (Leib, Leben oder persönliche Freiheit Dritter) abzuwehren . Maßnahmen mit dieser Zweckbestimmung dienen einem überragenden Gemeinwohlinteresse (vgl. BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 u. a., juris Rn. 100). Die Verwendung der Daten verletzt auch nicht den Kernbereich privater Lebensgestaltung. Allein das Wissen um die unterschiedlichen Aufenthaltsorte ermöglicht keine umfassende Kenntnis von die betroffene Person betreffenden Vorgängen höchstpersönlicher Art. Dies wäre allenfalls dann der Fall, wenn mit der Ortskenntnis jeweils auch die Kenntnis verbunden wäre, womit sich die Person an dem jeweiligen Ort beschäftigt. Vielmehr geht es hier nur darum, allein über den Aufenthaltsort zu dokumentierende Erkenntnisse im Hinblick auf eine konkrete Gefährdungssituation, z. B. an den ermittelten Standorten, erlangen zu können. Nach der Rechtsprechung des Bundesverfassungsgericht sind im Übrigen selbst höchstpersönliche Äußerungen nicht dem absolut geschützten Bereich persönlicher Lebensgestaltung zuzuordnen, wenn sich aus ihnen konkrete und erhebliche Gefahrenlagen für Dritte ergeben (BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 u. a., juris Rn. 122). Entsprechendes muss für bloße Aufenthaltsdaten gelten, die Hinweise auf eine Gefährdung Dritter geben, Opfer einer schweren Straftat gegen Leib, Leben oder die persönliche Freiheit zu werden. Satz 9 stellt im Übrigen klar, dass die erhobenen Daten über die in Nummer 1 bis 5 genannten Fälle hinaus mit Einwilligung der betroffenen Person auch für sonstige Zwecke verwendet werden dürfen. In Betracht kommt etwa eine Verwendung zur Aufklärung anderer Straftaten.

Absatz 4 Satz 1 enthält für die nach Absatz 3 Satz 1 erhobenen Daten eine grundsätzliche Löschungsfrist von zwei Monaten. Dieser Zeitraum ist notwendig, um klären zu können, ob die Daten für die in Absatz 3 Satz 9 genannten Zwecke noch benötigt werden. Eine über diese Frist hinausgehende Verwendung ist nur zulässig, wenn die Daten zu diesem Zeitpunkt bereits für einen der genannten Zwecke verwendet werden. Eine darüber hinausgehende Datenspeicherung lässt die Regelung nicht zu. Daten, die für die Zwecke nach Absatz 3 Satz 9 benötigt werden, können über den Zeitraum von zwei Monaten hinaus gespeichert bleiben und für diese Zwecke (weiter-)verwendet werden. Die weitere Verarbeitung richtet sich dann nach den allgemeinen Grundsätzen.

Nach Absatz 4 Satz 2 ist jeder Abruf der Daten zu protokollieren. Diese datenschutzrechtliche Vorgabe ermöglicht die nachträgliche Kontrolle, ob sich Kenntnisnahme und Verwendung der Daten im Rahmen der Zweckbindung nach Absatz 3 Satz 9 bewegt haben und durch eine berechtigte Stelle erfolgt sind. Ihr kommt insoweit auch eine präventive Wirkung zu.

Absatz 4 Satz 3 bis 5 statuieren eine Kennzeichnungs- und Sicherungspflicht für die erhobenen Daten und eine Protokollierungspflicht bezogen auf die jeweilige Maßnahme der elektronischen Aufenthaltsüberwachung, welche eine datenschutzrechtliche Überprüfung erleichtern und zudem die Einhaltung der Zweckbindung nach Absatz 3 Satz 9 gewährleisten sollen. Satz 6 und 7

orientieren sich stark am Wortlaut des Artikels 25 der EU-Richtlinie 2016/680. Nach Satz 8 sind die Protokolldaten nach vierundzwanzig Monaten zu löschen.

Bei Vorliegen von Gefahr im Verzug ist eine Entscheidung durch die Behördenleitung zulässig. Die richterliche Entscheidung ist unverzüglich nachzuholen. Der Richtervorbehalt ist der Tiefe des Grundrechtseingriffs geschuldet. Da es sich allerdings um eine offene Maßnahme und keine verdeckte Maßnahme handelt, besteht die Möglichkeit des Betroffenen, sein Handeln hierauf abzustimmen. Der Grundrechtseingriff ist insoweit weniger intensiv als im Falle einer verdeckten Maßnahme, bei der der Betroffene keine Möglichkeit hat, sein Verhalten anzupassen und insoweit deutlich mehr Informationen preisgibt. Zudem werden die Zugriffe auf die anfallenden Informationen umfangreich protokolliert und für den Fall einer etwaigen gerichtlichen Überprüfung bereitgehalten. Insoweit ist es angemessen, dass nicht nur die Behördenleitung, sondern auch andere höherrangige Mitglieder des Polizeivollzugsdienstes bei Gefahr im Verzug die elektronische Aufenthaltsüberwachung bereits beauftragen können und die richterliche Bestätigung nachgeholt wird.

Absatz 6 und 7 entsprechen den im Zusammenhang mit den anderen Gefahrenabwehrbefugnissen, die einer richterlichen Anordnung bedürfen, getroffenen Regelungen zum Inhalt des Antrags und zur gerichtlichen Anordnung.

Absatz 8 Satz 1 enthält eine Anordnung der sofortigen Vollziehung, um hierdurch die Voraussetzungen für die Verwaltungsvollstreckung zu schaffen und somit eine effektive Gefahrenabwehr zu gewährleisten. Damit kann offen bleiben, ob es sich um eine „unaufschiebbare“ Anordnung oder Maßnahme von Polizeivollzugsbeamten im Sinne des § 80 Absatz 2 Satz 1 Nummer 2 Verwaltungsgerichtsordnung handelt. Aus Gründen der Verhältnismäßigkeit wird die Dauer einer Anordnung auf höchstens drei Monate beschränkt. Nach Absatz 8 Satz 2 bedarf die Verlängerung der Maßnahme einer erneuten Anordnung. Auf diese Weise wird gewährleistet, dass es zu einer erneuten vollumfänglichen gerichtlichen Prüfung des Falls kommt. Da im Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit (FamFG) keine speziellen Regelungen zur elektronischen Aufenthaltsüberwachung vorhanden sind, gelangen die dortigen Vorschriften nur entsprechend zur Anwendung.

Zu Nummer 13 – § 33g (Schutz von Berufsgeheimnisträgern)

Der § 33g enthält eine Schutzvorschrift vor staatlichen Überwachungsmaßnahmen für Berufsgeheimnisträger, die sich auf ein Zeugnisverweigerungsrecht nach den §§ 53, 53a StPO berufen können. Die Regelungen gelten für die verdeckten Maßnahmen der Telekommunikationsüberwachung in §§ 33a bis 33d und für die elektronische Aufenthaltsüberwachung in § 33f. § 33g orientiert sich in seiner Ausgestaltung an § 62 Bundeskriminaltamtgesetz 2018 und §160a Strafprozessordnung.

Absatz 1 sieht ein striktes Überwachungsverbot nur für einen kleinen Personenkreis vor, für den der Gesetzgeber besonderen Schutzbedarf sieht. Für Geistliche, Strafverteidiger, Rechtsanwälte und Abgeordnete gilt nach Absatz 1 ein umfassendes Erhebungs- und Verwertungsverbot für alle Überwachungsmaßnahmen. Eine Unterscheidung zwischen Strafverteidigern und den in anderen Mandatsverhältnissen tätigen Rechtsanwälten ist als Abgrenzungskriterium für einen unterschiedlichen Schutz ungeeignet, weil die in Frage stehenden Überwachungsmaßnahmen nicht der Strafverfolgung, sondern der Gefahrenabwehr dienen, die Strafverteidigung also hier gerade nicht entscheidend ist. Strafverteidiger und Rechtsanwälte in anderen Mandatsverhältnissen sind daher gleichgestellt (siehe BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 u. a., juris Rn. 257).

Mit der Formulierung „voraussichtlich“ wird für die Polizeibehörden eine Prognoseentscheidung eröffnet. Wenn bereits die Wahrscheinlichkeit für ein Erfassen von schützenswerten Erkenntnissen besteht, darf die Maßnahme nicht angeordnet werden. Werden dennoch Erkenntnisse erlangt, so z. B. weil ein Ausschluss der Erhebung technisch nicht möglich ist, so dürfen diese jedoch nicht verwertet werden.

Um die Einhaltung der Löschungspflicht, vor allem aber um die spätere Nachvollziehbarkeit im Rahmen von Rechtsschutzbegehren Betroffener zu sichern, müssen gemäß § 33g Absatz 1 Satz 4 sowohl die Tatsache der Erlangung unverwendbarer Erkenntnisse als auch die Löschung entsprechender Aufzeichnungen in den Akten festgehalten werden.

Für den Fall der zufälligen Betroffenheit des nach Absatz 1 Satz 1 geschützten Kreises von Berufsgeheimnisträgern durch eine nicht gegen diesen gerichtete und daher zulässige Maßnahme ordnet Absatz 1 Satz 5 die entsprechende Geltung des Verwertungsverbots sowie der Löschungs- und Dokumentationspflicht an. Erbringt also die gegen eine andere Person gerichtete Maßnahme Erkenntnisse, die von einem der genannten Berufsgeheimnisträger erlangt wurden und über die dieser das Zeugnis verweigern dürfte, greift auch insoweit das Verwertungsverbot ein.

Absatz 2 schließt – in enger Anlehnung an § 160a Absatz 2 Strafprozessordnung – die Überwachung von Ärzten, Journalisten und anderen Berufsgeheimnisträgern nach Maßgabe einer Abwägung im Einzelfall aus. Insoweit eröffnet Absatz 2 verfassungsrechtlich zulässig (BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 u. a., juris Rn. 258) weiter gehende Befugnisse gegenüber den hier genannten Personengruppen als bei der strikten Regelung des Absatzes 1. Bei der hier vorzunehmenden Abwägung sind die Grundrechte der Betroffenen angemessen zu gewichten. Dabei ist die Abwägung durch den Verhältnismäßigkeitsgrundsatz strukturiert. In Entsprechung zu § 160a Absatz 2 Satz 1, 2. Halbsatz Strafprozessordnung gebietet die Verfassung insoweit die Vermutung, dass von einem Überwiegen des Interesses der Polizeibehörden an der Erhebung der Daten in der Regel nicht auszugehen ist, wenn die Maßnahme nicht der Abwehr einer erheblichen Gefahr dient (vgl. BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 u. a., juris Rn. 256). Insoweit kommt eine Überwachung nur ausnahmsweise und nur unter sehr engen Voraussetzungen in Betracht. Der Anordnung muss zu entnehmen sein, welche besonderen Gründe für die Überwachung der in Absatz 2 genannten Personen sprechen.

Ein Anspruch auf umfangreicheren Schutz für Medienvertreter ergibt sich insbesondere nicht aus Artikel 5 Absatz 1 Satz 2 Grundgesetz (vgl. BVerfG, Urteil vom 12.03.2003 – 1 BvR 330/96 u. a., juris Rn. 116, 120). Weitere Grenzen ergeben sich auch nicht aus Artikel 3 Absatz 1 Grundgesetz. Der Gesetzgeber darf die Zuerkennung eines strengeren Schutzes vor Überwachungsmaßnahmen als Ausnahme für spezifische Schutzlagen verstehen, hinsichtlich derer er einen erheblichen Einschätzungsspielraum hat (BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 u. a., juris Rn. 258.). Die Anerkennung einer solchen besonderen Schutzbedürftigkeit von Geistlichen und Abgeordneten gegenüber anderen Berufsgruppen ist verfassungsrechtlich nicht zu beanstanden. Eine Pflicht zur Ausweitung dieses besonders strikten Schutzes auf weitere Gruppen kann nicht abgeleitet werden (vgl. BVerfG, Beschluss vom 12.10.2011 - 2 BvR 236/08 u. a., juris Rn. 259, 263). Unberührt bleibt, dass in die für die anderen Berufsgeheimnisträger gebotene Abwägung auch unter Berücksichtigung des Artikel 12 Absatz 1 Grundgesetz die Vertrauensbedürftigkeit der jeweiligen Kommunikationsbeziehungen im jeweiligen Einzelfall maßgeblich einzufließen hat und darüber hinaus eine Überwachung – etwa für psychotherapeutische Gespräche – auch unter dem Gesichtspunkt des Kernbereichs privater Lebensgestaltung ausgeschlossen sein kann (BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 u. a., juris Rn. 258).

Absatz 3 erweitert den Anwendungsbereich auf die sog. Berufshelfer, sofern ihnen das Zeugnisverweigerungsrecht zusteht.

Absatz 4 entspricht dem berechtigten Interesse an einer effektiven Gefahrenabwehr. Danach gilt das Erhebungs- und Verwertungsverbot nicht, wenn bestimmte Tatsachen die Annahme rechtfertigen, dass die zeugnisverweigerungsberechtigte Person für die Gefahr verantwortlich ist.

Zu Nummer 14 – Überschrift Vierter Teil

Die Änderung in Nummer 15 mit der Neuaufnahme eines Paragraphen, der weder dem dritten noch dem bisherigen vierten Teil zuzuordnen ist, erfordert die Einfügung eines neuen Vierten Teils.

Zu Nummer 15 – § 84 (Strafvorschriften)

Insofern, als das Strafrecht nach Artikel 74 Absatz 1 Nummer 1 Grundgesetz der konkurrierenden Gesetzgebung unterfällt, ist der Landesgesetzgeber gemäß Artikel 72 Absatz 1 Grundgesetz zu einer Regelung befugt, soweit und solange der Bundesgesetzgeber von seiner Regelungsbefugnis keinen Gebrauch gemacht hat. Da der Bund im Rahmen seiner Vorschriften eine Strafbarkeit lediglich für Verstöße gegen die bundesrechtlichen Anordnungen normiert, sind die Landesgesetzgeber nicht daran gehindert, ihrerseits für Verstöße gegen Landesrecht Strafen vorzusehen. Die durch den Landesgesetzgeber zu verhängende Freiheitsstrafe beträgt nach Artikel 3 Absatz 1 Nummer 1 Einführungsgesetz zum Strafgesetzbuch maximal zwei Jahre oder Geldstrafe.

In Anlehnung an § 39 Bundeskriminalamtgesetz 2018 erfolgt die Normierung einer Strafbarkeit von Verstößen. Diese Vorschrift ist erforderlich, da die elektronische Aufenthaltsüberwachung nach § 33f und die Einhaltung von Aufenthaltsanordnungen und Kontaktverboten nach § 14b von der Mitarbeit der Personen abhängig sind, denen gegenüber sie angeordnet werden. Diese Kooperationsbereitschaft ist bei sog. Gefährdern aber fraglich. Der Staat erhält hierdurch die Möglichkeit, etwaige Verstöße unmittelbar zu sanktionieren und somit den Befugnissen mehr Nachdruck zu verschaffen. Die Einstufung eines Verstoßes gegen die genannten Regelungen als Ordnungswidrigkeit zu diesem Zweck wäre nicht ausreichend.

Zu Nummer 16 bis 22 – redaktionelle Anpassungen

Die Änderungen in Nummer 14 und 15 erfordern die Änderung der Überschrift zum bisherigen Vierten Teil sowie die Änderung der Bezeichnungen der bisherigen §§ 84 bis 89.

Zu Artikel 2

Die Bestimmung regelt das Inkrafttreten des Gesetzes.