Bericht

der länderoffenen Arbeitsgruppe des AK IV

Zusammenarbeit der Verfassungsschutzbehörden des Bundes und der Länder -

Schaffung eines harmonisierten Rechtsrahmens mit wirksamen Befugnissen

---

Stand: 29.08.2017

Inhalt

Anlagen

Anlage 1: Allgemeine Befugnis zur Datenverarbeitung

Anlage 2: Allgemeine Regelungen zum Einsatz nachrichtendienstlicher Mittel

Anlage 3: Einsatz verdeckter Mitarbeiter und von Vertrauensleuten

Anlage 4: Eingriffe in Art. 10 GG

Anlage 5: Verdeckter Eingriff in Informationstechnische Systeme

Anlage 6: Wohnraumüberwachung

Anlage 7: Besondere Auskunftsverlangen, Mitwirkungspflichten

Anlage 8: Alternativvorschläge NI zu den Anlagen 2, 3 und 7

1. Auftrag und Arbeitsweise der Arbeitsgruppe

Der AK IV hat in seiner Sitzung am 04./05. April 2017 zu TOP 5 „Zusammenarbeit der Verfassungsschutzbehörden des Bundes und der Länder“ unter Ziffer 2 beschlossen:

> *„Der AK IV ist der Auffassung, dass die effektive Zusammenarbeit der Verfassungsschutzbehörden insbesondere im Bereich des gewaltbereiten Extremismus einen harmonisierten Rechtsrahmen mit wirksamen Befugnissen erfordert. Er begrüßt, dass das BMI zu einer länderoffenen Arbeitsgruppe einlädt, die die bestehenden gesetzlichen Befugnisse von Bund und Ländern analysiert und Anpassungs- bzw. Regelungsbedarfe beschreibt.*“

Die IMK hat hierauf in ihrer 206. Sitzung am 12./14. Juni 2017 zu TOP 34 unter Ziffer 2 beschlossen:

> *„Die IMK ist der Auffassung, dass die effektive Zusammenarbeit der Verfassungsschutzbehörden insbesondere im Bereich des gewaltbereiten Extremismus einen harmonisierten Rechtsrahmen mit wirksamen Befugnissen erfordert. Sie begrüßt, dass der AK IV eine Arbeitsgruppe einrichtet, die die bestehenden gesetzlichen Befugnisse von Bund und Ländern analysiert und Anpassungs- bzw. Regelungsbedarfe beschreibt.“*

An der Arbeitsgruppe nahmen neben dem federführenden BMI teil: BW, BY, BE, HH, MV, NI, NW, RP sowie das BfV.

Die Arbeitsgruppe hat Übermittlungsbefugnisse von ihrer Untersuchung ausgenommen, da die IMK einen gesonderten Auftrag[1] zur Prüfung etwaigen Handlungsbedarfs beim Informationsfluss zwischen den Sicherheitsbehörden erteilt hat. Den Schwerpunkt ihres Auftrags hat die Arbeitsgruppe in den Erhebungsbefugnissen gesehen. Ergänzend hat sie sich mit Besonderheiten beim Umgang mit personenbezogenen Daten Minderjähriger befasst. Ansonsten hat sie zu weiteren Verarbeitungsregelungen keinen prioritären Prüfungs- oder Handlungsbedarf erkannt.

---

[1] Nr. 3 im o.a. IMK-Beschluss: „Die IMK hält eine Intensivierung des Informationsaustauschs zwischen den Sicherheitsbehörden zur effektiven Terrorismusabwehr für unverzichtbar. Sie stellt fest, dass das sogenannte informationelle Trennungsprinzip der informationellen Zusammenarbeit der Sicherheitsbehörden einen engen Rahmen vorgibt. Sie nimmt zur Kenntnis, dass der AK IV unter Beteiligung des AK II eine Arbeitsgruppe mit dem Prüfauftrag eingerichtet hat, ob in Folge dessen oder aus anderen Gründen der notwendige Informationsfluss erschwert oder verhindert wird und ob sich daraus Handlungsbedarf ergibt.“

Die Arbeitsgruppe tagte am 18./19. Juni und am 31. Juli 2017. Der ersten Sitzung lag eine Auswertung der geltenden Regelungen in den Verfassungsschutzgesetzen von Bund und Ländern und deren Analyse zugrunde, ferner eine grobe Sichtung einschlägiger Verfassungsrechtsprechung sowie erste Überlegungen für Eckpunkte und konkrete Modellregelungen wirksamer Erhebungsbefugnisse. Die Ergebnisse der ersten Sitzung hatte das federführende BMI in einen Berichtsentwurf sowie einer Fortschreibung der Unterlagen umgesetzt, die Gegenstand der zweiten Besprechung und einer nachfolgenden Schlussabstimmung im schriftlichen Umlaufverfahren waren. Die Ergebnisse zu den Regelungsvorschlägen sind als Anlagen 1 bis 8 beigefügt, wobei Anlage 8 von NI präferierte Alternativvorschläge zu einzelnen Paragraphen der Anlagen 2, 3 und 7 enthält.

Gemäß dem Auftrag des AK IV war Bewertungsmaßstab die Wirksamkeit der Befugnisse, so dass die Arbeitsgruppe ihre Würdigung vorrangig auf praktische Anforderungen und fachlichen Bedarf bezogen hat. Sie war sich dabei bewusst, dass eine abgewogene politische Entscheidung des Gesetzgebers sachgerecht weitere Aspekte berücksichtigt. Dies schließt gleichermaßen materiell eine vertiefende verfassungsrechtliche Würdigung ein wie auch verfahrensbezogen die Beteiligung der unabhängigen Datenschutzbehörden. Eine derart komplexe Befassung der Arbeitsgruppe hätte indes den Auftrag überdehnt und wäre im gegebenen Rahmen weder ebenengerecht noch operabel gewesen. Insoweit versteht sich der Bericht nicht als abschließende Untersuchung, sondern als fachlicher Beitrag zu einer breiteren rechtspolitischen Diskussion. Sie ist insoweit dem vom AK II bereits praktizierten und von der IMK[2] zur Kenntnis genommen Vorgehensmodell für „Gesetzgeberische Handlungsempfehlungen im Zusammenhang mit islamistischem Terrorismus“ gefolgt, die ebenfalls zunächst aus fachlicher Perspektive Befugnisvorschläge (etwa zur „Online-Durchsuchung“) enthalten, welche ebenso vor einer Umsetzung weiterer politischer Würdigung bedürfen. Dabei liegt politisch nahe, dass Länder, die erst jüngst umfassende Änderungen ihrer Verfassungsschutzgesetze vorgenommen haben (so BY und NI, mit unterschiedlicher Ausrichtung), möglicherweise eher zurückhaltend bei neuerlichen Änderungen sein könnten. Die Arbeitsgruppe war sich dabei bewusst, dass dies in einem gewissen Spannungsverhältnis zum Harmonisierungsauftrag steht. Angesichts deutlich unterschiedlicher politischer Gewichtung verschiedener relevanter Aspekte in Bund und Ländern erscheint die Harmonisierung indes eher als prozesshaftes Optimierungsziel operabel und derzeit kaum in einem Schritt erreichbar.

2. Allgemeine Erläuterungen zu den Vorschlägen

2.1. Systematik/Terminologie

Die Arbeitsgruppe hat im Interesse der angestrebten Harmonisierung konkrete Musterregelungen entworfen (Anlagen). Vorgeschlagen werden Regelungen für:

[2] Beschluss zu TOP 52 in der Frühjahrsitzung am 12. bis. 14. Juni 2017.

- Allgemeine Regelungen je für die Datenverarbeitung und den Einsatz nachrichtendienstlicher Mittel,
- Einsatz von Verdeckten Mitarbeitern und Vertrauensleuten,
- Eingriffe in Art. 10 GG (Verkehrs- und Inhaltsdaten),
- Verdeckter Eingriff in informationstechnische Systeme,
- Wohnraumüberwachung und
- Mitwirkungspflichten Dritter, einschließlich besondere Auskunftsverlangen gegenüber Unternehmen.

Die Vorschläge sind abstrahiert modellhaft. Die Begrifflichkeiten orientieren sich einerseits an der allgemeinen Datenschutzterminologie (bereits in der Fassung des DSAnpUG-EU) andererseits an den Begriffen einschlägiger - auch untergesetzlicher - Bundesvorschriften (Beispielsweise „verdeckte Ermittlungen“). Soweit die Vorschläge aufgegriffen werden, bleiben die Inhalte ggf. an die Regelungssystematik und Begrifflichkeit des jeweiligen Gesetzes anzupassen. Perspektivisch könnte allerdings auch eine terminologische, letztlich auch regelungssystematische Harmonisierung anzustreben sein. Im Vordergrund steht aber der Regelungsinhalt mit wirksamen Befugnissen.

2.2. Modularer Ansatz der Musterregelungen

Die Vorschläge beruhen in doppelter Hinsicht auf dem Ansatz, Basismodule zu formulieren, die je nach entsprechender Ausrichtung des Landes-/Bundesrechts ergänzt werden:

- Zum einen werden zunächst Kernmodule formuliert, die aus dem rein fachlichen Blickwinkel und mit Betonung der Effektivität der Aufgabenwahrnehmung entworfen sind. Dies ist ggf. - wie oben ausgeführt - mit weiteren Belangen in Einklang zu bringen.

  Beispielhaft sind hier die Mitteilungspflichten zu nennen. Da die Betroffenen verdeckter Maßnahmen durch die Nachrichtendienste des Eingriffs in ihre Rechte nicht gewahr sind, bestehen bereits jetzt Regelungen, die die Nachrichtendienste verpflichten, im Nachgang den Betroffenen hierrüber in Kenntnis zu setzen, soweit operative Interessen nicht mehr berührt sind. Die Modellregelung X+10 Abs. 1 enthält einen vorgeschlagenen Kranz an Maßnahmen, nach denen eine Mitteilung an den Betroffenen zu erfolgen hat. Diese könnte je nach politischer Abwägung auf zusätzliche ND-Mittel erweitert werden.

- Die Vorschläge basieren auf dem zurückhaltenden Ansatz gesetzlicher Regelungsdichte, die gesetzgeberische Entscheidungen auf besonders Wesentliches beschränkt, um Entwicklungsoffenheit (in technischer und methodischer Hinsicht) zu wahren und der Verwaltung die nötige Vollzugsflexibilität zu belassen. Beispielsweise sind ergänzend zu den allgemeinen Regelungen über den Einsatz nachrichtendienstlicher Mittel nur solche Mittel noch besonders geregelt, die in der gewaltenteilenden Demokratie spezielle Vorgaben des Gesetzgebers erfordern (wegen des Eingriffs in grundrechtlich besonders verbürgte Privatheitsrechte [Art. 10, 13 GG] bzw. besonderer politischer Sensitivität [Vertrauensleute, Verdeckte Mitarbeiter]).

  Einige Länder gehen seit vielen Jahren den gegenteiligen Weg, indem die nachrichtendienstlichen Mittel abschließend geregelt sind. Auch bei einer umfassenden Gesetzessystematik, wonach beispielsweise der konkrete Einsatz eines Mittels aber nicht dessen grundsätzliche Befugnis eine Verschlusssache darstellt, können die Vorschläge genutzt und die Regelungen in das Regelungskonzept der jeweiligen Verfassungsschutzgesetze homogen eingefügt werden.

Die Arbeitsgruppe hat sich angesichts der Vorgabe „wirksamer“ Befugnisse vorrangig an Anforderungen effektiver und effizienter Aufgabenwahrnehmung und dem Schutz der darin angelegten Gemeinwohlinteressen orientiert. Ausgehend von §§ 9-21 NVerfSchG sieht NI in den Regelungen der Anlage 8 vorzugswürdige Alternativen zu den Anlagen 2, 3 und 7, wodurch aus dortiger Sicht rechtsstaatlichen Anliegen, etwa dem Datenschutz, besser Rechnung zu tragen sei, ohne die wirksame Aufgabenwahrnehmung zu hindern. Nach überwiegender Auffassung in der Arbeitsgruppe hingegen sollte aus fachlicher Sicht - dem Optimierungsziel wirksamer Befugnisse folgend - von Einschränkungen eher zurückhaltend Gebrauch gemacht werden, da aus dieser Sicht auch die Anlagen 2, 3 und 7 bereits ausgewogen erscheinen.

3. Einzelfragen

3.1. Zur Bindungswirkung des BKAG-Urteils des BVerfG

Die Rechtskraft der Entscheidung des BVerfG vom 20.04.2016 ist auf den Entscheidungsgegenstand, das BKA-Gesetz begrenzt. Jenseits rechtlicher Bindung enthält das Urteil gleichwohl wichtige allgemeine Überlegungen zu heimlichen Überwachungsmaßnahmen. Das BVerfG hat die Gelegenheit genutzt, Aussagen genereller Bedeutung für das Verhältnis von Sicherheit, Freiheit und Datenschutz zu treffen.

Nach überwiegender Auffassung in der Arbeitsgruppe gibt es aber gute Gründe, gerade wegen informationeller Trennung von Nachrichtendiensten und Polizei die vom Gericht

zur Polizei angestellten Überlegungen nicht ohne weiteres eins zu eins auf Nachrichtendienste zu übertragen. Diese Trennung bezweckt gerade, die Informationsbreite der Gefahrerforschung zu filtern und zu validieren, bevor Informationen in staatlichen Aktionen wirksam werden. Dabei wird Privatsphäre ausgefiltert, Erkenntnisse werden auf Sozialbezug komprimiert und diese wiederum in ihrer Qualität durch Verifizierung, Anreicherung und Verdichtung gesichert. Die Risiken einer Fehlsteuerung staatlicher Zwangsgewalt werden also in einer vorgelagert abgeschotteten Prozessphase - organisatorisch gesichert - minimiert, bevor die Information durch einen gesonderten Eingriff nach Maßgabe weiterer (Übermittlungs-)Schwellen für solche Hoheitsgewalt verfügbar wird. Der so strukturierte Prozess ist grundrechtsschonender und fordert demgemäß weniger restriktive materielle Erhebungsschwellen und weniger zusätzliche Verfahrenssicherungen.

Nach einer anderen in der Arbeitsgruppe vertretenen Auffassung ist die Tendenz des BVerfG dementgegen eindeutig, wonach ein Grundrechtseingriff durch den Verfassungsschutz keine nennenswert andere Qualität hat, als ein vergleichbarer Eingriff durch die Polizei oder eine andere hoheitlich tätige Stelle. Nach dieser Auffassung sollten mithin die Wertungen des Bundesverfassungsgerichtes auch auf das Recht der Nachrichtendienste übertragen werden, um verfassungsfeste Regelungen zu schaffen. Insbesondere solle man danach die Eingriffshürden angleichen und verstärkt verfahrenssichernde Elemente integrieren.

Einigkeit bestand in der Arbeitsgruppe, dass das Urteil mindestens in einigen Punkten auch Änderungen im künftigen Nachrichtendienstrecht anstößt. Dies betrifft vornehmlich einen materiell erweiterten Schutz des Kernbereichs privater Lebensgestaltung (und die Gleichbehandlung aller Mandantenverhältnissen von Rechtsanwälten). Rechtspolitisch ist die vom Gericht nahe gelegte Kategorisierung im Sinne einer Clusterbildung von einerseits „Gefahren-“, andererseits „Maßnahmeklassen“ rechtsvereinfachend[3].

3.2. Neubewertung der „Online-Datenerhebung“

Diese Clusterbildung schließt insbesondere die vom Gericht vorgenommene normative Synchronisierung des Eingriffs in informationstechnische Systeme mit der Wohnraumüberwachung ein. Dem folgend sehen die dies betreffenden Musterregelungen einheitliche Einsatzschwellen vor.

[3] zur Strafverfolgung bezieht sich das BVerfG auf die Straftatenkategorien „erheblich“/“schwer“/“besonders schwer“ mit korrespondierden Maßnahmekategorien abgestufter Eingriffsintensität (Rn. 107), zur Gefahrenabwehr legt es eine entsprechende Clusterung nahe (Rn. 108: „ist nicht gehindert“), die die betreffenden Maßnahmekategorien je einheitlich an abgestufte Gefahrenschwellen (also: erhebliche/schwere/besonders schwere) knüpft. In den Anlagen wird dies aufgegriffen mit dem Bezug auf BO von erheblicher Bedeutung (§ X Abs. 3 Satz 2) und - komplementär zu § 100a Abs. 2 StPO bzw. § 100c Abs. 2 StPO - schwere bzw. besonders schwere Gefahren, die durch besondere Schutzgüter oder modi operandi qualifiziert werden (§ X+3 Abs. 1 bzw. § X+4 Abs. 1).

Der Befugnistatbestand ist dabei in zwei Alternativen formuliert, die einerseits eine allgemein formulierte dringende Gefahr (für herausragende Rechtsgüter) bezeichnen und andererseits diese leitbildhaft durch Anknüpfung an bestimmte Straftatenverdachte konkretisieren. Letzteres hat sich in der Anwendungspraxis des G 10 bewährt und wird daher im Interesse der Rechtsklarheit hier ergänzend aufgegriffen (zumal das Gericht seine Erwägungen zu konkretisierten Gefahren seinerseits auf drohende Straftaten bezieht).

3.3. Bundeseinheitliche Befugnisse zum Eingriff in Art. 10 GG - Verhältnis zum G10

Der Bundesgesetzgeber hat 1968 und seitdem vom Bundesverfassungsgericht unbeanstandet im G 10 TKÜ-Befugnisse auch für die Landesverfassungsschutzbehörden geregelt. Insoweit besteht innerhalb des Verfassungsschutzverbundes bereits jetzt Rechtseinheit. Es erscheint nicht stringent, dass der Vollzugriff auf das geschützte Rechtsgut mittels TKÜ durch den Bundesgesetzgeber für alle bundesdeutschen Verfassungsschutzbehörden einheitlich im G 10 geregelt ist, während der geringfügigere Eingriff durch Erhebung von Verkehrsdaten dagegen nur im BVerfSchG und damit nur für den Bund. Kompetenzrechtliche Erwägungen können hierfür keine Rolle spielen, so dass es sinnvoll erscheint, dass der Bundesgesetzgeber zusammen mit einer grundlegenden Novellierung des G10 Rechtseinheit schafft. Dies schließt die Erhebung von Verkehrsdaten (auch die nach § 113b TKG gespeicherten) ein.

3.4. Zuständigkeit der G-10-Kommission

Im Sinne einer Grundrechtssicherung durch Verfahren sehen die Musterregelungen zu besonders schwerwiegenden nachrichtendienstlichen Mitteln die vorherige Entscheidung der G 10-Kommission als unabhängige Stelle vor. Für die Wohnraumüberwachung ist in Art. 13 Abs. 4 GG allerdings ausdrücklich ein Richtervorbehalt vorgesehen. Die Arbeitsgruppe hat dies als „Richter im funktionellen Sinne“ verstanden und daher die Befassung der G 10-Kommission als sachnahes Gremium vorgesehen. Der durch die Kommission gebotene Rechtsschutz ist nach der Rechtsprechung des BVerfG materiell und verfahrensmäßig der gerichtlichen Kontrolle gleichwertig. Die G 10-Kommission besitzt aufgrund der Einbindung in die G 10-Verfahren zur Arbeitsweise der Nachrichtendienste (einschließlich Grundlagen technischer Überwachung) besondere Fachexpertise. Eine Bündelung der Kontrolle unterschiedlicher Maßnahmen gegen dieselben Zielpersonen bei einer Kontrollinstanz schafft eine besondere Schutzqualität auch hinsichtlich additiver Effekte. Mit der Zuständigkeit der G 10-Kommission wird zugleich ein besonderes Kontrollregime (mit Entscheidungskompetenz) auch für die weitere Datenverarbeitung etabliert. All dies spricht für den Regelungsansatz der Arbeitsgruppe, der gleichwohl im Besonderen noch verfassungsrechtlicher Prüfung bedürfen wird.

4. Verarbeitung von Daten minderjähriger Personen

Mit Ausnahme des bayerischen Landesgesetzes sehen alle Verfassungsschutzgesetze vor, dass die im Zusammenhang mit der Aufgabenerfüllung erhobenen Daten minderjähriger Personen unter 14. Jahren nicht in Dateien gespeichert werden dürfen.

Informationstechnik ist zentrales Werkzeug für die Informationssammlung und analytische Arbeit der Verfassungsschutzbehörden. Mit dem NADIS-Wissensnetz endet der Informationsverbund der Verfassungsschutzbehörden nicht an der Landesgrenze. Es ist notwendig, länderübergreifend die Aktivität von relevanten Personen zu verfolgen, zusammenzuführen und verfügbar zu machen. Technik erleichtert zugleich effektiven Datenschutz, indem sie beispielsweise automatisch auf den Ablauf von Nachprüfungs- und Löschungsfristen erinnert oder Zugriffe protokolliert.

In der Arbeitsgruppe wurde daher überwiegend dafür plädiert, die Einschränkung der Dateispeicherung zu minderjährigen Personen zu streichen. Ein Mitglied sieht aber speziell zu dieser Personengruppe Besonderheiten, die denen angemessene - besondere - Befugnisbeschränkungen erfordern. Im Folgenden werden die unterschiedlichen Meinungen neben einander gestellt.

4.1. Votum für eine Beibehaltung der derzeitigen Rechtslage

Die Erhebung und Speicherung von personenbezogenen Daten bereits von Kindern ist für die Aufgabe des Verfassungsschutzes nicht erkennbar notwendig. Diese besteht in der Vorfeldaufklärung und Strukturerkennung.

In Fällen konkreter Gefahrenabwehr und Strafverfolgung ist die Polizei zur Erhebung von Daten befugt. So auch bei dem seitens der Gegenposition angesprochenen Minderjährigen in Ludwigshafen. Dieses Beispiel für eine generelle Gefährlichkeit von Kindern und Jugendlichen zu bemühen, ist verfehlt. Den Sicherheitsbehörden sind ganz offensichtlich nicht die Hände gebunden. Es verdeutlicht vielmehr, dass keine Sicherheitslücke besteht. Deswegen ist nicht erkennbar, wohin diese Forderung eigentlich führen soll.

Der Ansatz, die Beobachtung von Kindern im schlimmsten Falle schon auf das Säuglingsalter auszuweiten, verkennt das tatsächliche Problem. Ursache radikalisierter Kinder und Jugendlicher sind regelmäßig Erwachsene. Der Schwerpunkt des Verfassungs-

schutzes darf daher nicht auf den Kindern liegen. Diese sind selbst Opfer geworden. Vielmehr muss im Rahmen einer geeigneten Prävention der Fokus auf der Verhinderung von Radikalisierung liegen. Wie bereits das Bundesverfassungsgericht festgestellt hat, bedarf ein effektiver Jugendschutz zunächst wirkungsvoller Präventivmaßnahmen, um erkannte Gefahrenquellen rechtzeitig auszuschalten. Diese können sodann durch geeignete repressive Maßnahmen ergänzt oder verstärkt werden (BVerfGE 30, 336, 350). Kinder vor Vollendung des 14. Lebensjahres der Speicherung und in letzter Konsequenz sogar der Beobachtung durch den Verfassungsschutz auszusetzen, widerspricht dem.

Die Datenerhebung und Speicherung muss sich an der altersgemäßen Entwicklung orientieren, ohne Sicherheitsbedürfnisse zu ignorieren. Hierfür bedarf es eines abgestuften Systems, wie es in Niedersachsen geregelt ist. Dort ist eine Erhebung personenbezogener Daten minderjähriger Personen, die das 14. Lebensjahr noch nicht vollendet haben, ausnahmslos unzulässig. Bei Personen, die das 14. Lebensjahr, aber noch nicht das 16. Lebensjahr vollendet haben, ist eine Erhebung von Daten nur unter strengen Vorgaben (z.B. tatsächliche Anhaltspunkte für eine terroristische Straftat nach § 3 Abs. 1 Art.10 – Gesetz oder Abwehr einer Gefahr für Leib und Leben) erlaubt. Ab Vollendung des 16. Lebensjahres wird diese Schranke nochmals gelockert. Nunmehr ist eine Erhebung und Speicherung bei Gewaltbezug oder einer herausgehobenen Stellung des Jugendlichen in dem Objekt möglich. Ab Vollendung des 18. Lebensjahrs ist die Datenerhebung und Speicherung uneingeschränkt zulässig. Durch dieses System der Anknüpfung an die Entwicklung und die Handlungen der Minderjährigen wird ein angemessener Ausgleich zwischen dem Schutz der Jugendlichen und dem öffentlichen Sicherheitsbedürfnissen gewährleistet

4.2. Abschaffung von Altersgrenzen zur Datenspeicherung

In der Vergangenheit sind - in Einzelfällen - Minderjährige als Mitglied in einschlägigen Bestrebungen, bei Ausreiseversuchen in die Operationsgebiete ausländischer Terrorvereinigungen, sowie durch - bislang - vergebliche Versuche zum Einsatz von USBV aufgefallen, dies auch unterhalb der Altersgrenze von 14 Jahren. Auch sehr junge Menschen sind nicht nur körperlich in der Lage zu diesen Taten, sie sind - aufgrund ihrer fehlenden Erfahrung sowie der sich oftmals episodenhaft vollziehenden Persönlichkeitsentwicklung - besonders anfällig für die falschen Versprechungen terroristischer Vereinigungen, von denen sie teils gezielt als vulnerable Gruppe angesprochen werden. Daher verdienen Kinder und Jugendliche den besten Schutz der Gesellschaft.

Es ist daher sachgerecht und nach geltendem Recht Aufgabe der Verfassungsschutzbehörden auch Informationen über Minderjährige zu sammeln, die von extremistischen Bestrebungen für ihre Zwecke instrumentalisiert werden. § 11 Abs. 1 Satz 2 BVerfSchG unterbindet jedoch (in Verbindung mit § 6 Abs. 2 Satz 2 BVerfSchG auch für das NADIS WN), dass Daten unterhalb der Mindestalterschwelle von 14 Jahren in den vorhandenen

Dateien gespeichert werden. Damit scheidet ein effektiver Wissenstransfer von Behörde zu Behörde aus, länderübergreifende Zusammenhänge bleiben unter Umständen unerkannt. Im Extremfall werden Vorbereitungen für eine Ausreise in das Jihadgebiet nicht erkannt. Dies gefährdet vor allem das Kind selbst, welches möglicherweise ohne oder gegen den Willen seiner Eltern Deutschland verlässt, um sich in ein Kriegsgebiet zu begeben, in denen es größeren Gefahren ausgesetzt ist, als die Einschränkung der informationellen Selbstbestimmung es je könnte.

Regelungen, die an das Alter potentieller Täter anknüpfen, sind im Gefahrenabwehrrecht generell unüblich und auch wesensfremd, da bei der Gefahrenbeseitigung Fragen der Schuld bzw. Einsichtsfähigkeit keine Rolle spielen. So enthalten die Polizeigesetze konsequenter Weise keine Mindestalterregelung für Dateispeicherungen (sondern lediglich spezielle Aussonderungsprüffristen, die auch im Verfassungsschutzrecht eingeführt - vgl. § 11 Abs. 2 BVerfSchG - und unbestritten sachgerecht sind, ggf. bei Aufhebung der Altersgrenze komplementär auch zu verschärfen wären).

Eine Mindestalterregelung zur Dateispeicherung erscheint danach - auch - im Verfassungsschutzrecht sachwidrig. Vor allem gefährdet eine solche Regelung gerade diejenigen, die sie schützen soll: die Betroffenen selbst. Zu diesen stehen ohnehin mangels Strafmündigkeit keine Repressivmaßnahmen, sehr wohl aber nötige Maßnahmen der Jugendhilfe im Raum. Dem ist nicht gedient, wenn der Staat sich zu Gefährdungslage und Handlungsbedarf blind macht. Dabei ist es nicht Aufgabe von Jugendämtern, Feldforschung im extremistischen Milieu zu betreiben. Umgekehrt ist gerade Aufgabe der Verfassungsschutzbehörden, die jeweils zuständigen Stellen bei deren Präventionsaufgaben informationell durch Erkenntnisse über extremistische Bestrebungen zu unterstützen.

5. Beschlussvorschlag[4]

Die Arbeitsgruppe schlägt dem AK IV vor, wie folgt zu beschließen:

1. Der AK IV nimmt den Bericht der Arbeitsgruppe „Harmonisierung wirksamer Befugnisse der Verfassungsschutzbehörden“ (Stand: …) zur Kenntnis.

2. Er stellt fest, dass der Bericht gesetzgeberische Optionen aufzeigt, um die Aufklärung extremistischer und terroristischer Bestrebungen zu verbessern. Grundlage dafür ist die Harmonisierung der wesentlichen Regelungen in Bund und Ländern. Er sieht darin eine gute fachliche Grundlage für politische Überlegungen zur Harmonisierung des Rechtsrahmens der Verfassungsschutzbehörden des Bundes und der Länder.

3. Der AK IV bekräftigt, dass die Harmonisierung des Rechtsrahmens nur mit wirksamen Befugnissen eine sinnvolle Zielstellung ist.

4. Er bittet die IMK, wie folgt zu beschließen:

   4.1. Die IMK nimmt den Bericht „Harmonisierung wirksamer Befugnisse der Verfassungsschutzbehörden“ (Stand: …) sowie den Beschluss des AK IV vom … zur Kenntnis.

   4.2. Sie stellt fest, dass der Bericht gesetzgeberische Optionen aufzeigt, um die Aufklärung extremistischer und terroristischer Bestrebungen zu verbessern. Grundlage dafür ist die Harmonisierung der wesentlichen Regelungen in Bund und Ländern. Sie empfiehlt Bund und Ländern, den Bericht in Überlegungen zur Novellierung ihrer Verfassungsschutzgesetze einzubeziehen.

   4.3. Sie ist der Auffassung, dass die Harmonisierung des Rechtsrahmens nur mit wirksamen Befugnissen eine sinnvolle Zielstellung ist.

Die Arbeitsgruppe schlägt ferner vor, nach einem IMK-Beschluss über diesen Bericht - abhängig vom Inhalt des Beschlusses - im AK IV zu erwägen, eine Folgearbeitsgruppe einzurichten, die ergänzend Harmonisierungsvorschläge auch zu weiteren Standardregelungen der Verfassungsschutzgesetze erarbeitet, speziell in Bezug auf Aufgaben und Definitionen, ggf. auch - unter Einbezug der Erkenntnisse der „AG Trennungsprinzip“ (oben Fn. 1) - in Bezug auf Übermittlungsvorschriften.

---

[4] Der Beschlussvorschlag orientiert sich am Beschluss der 206. IMK am 12./14. Juni 2017 zu TOP 52 „Gesetzgeberische Handlungsempfehlungen im Zusammenhang mit islamistischem Terrorismus“ und dem zu Grunde liegenden Beschlussvorschlag des AK II

1 Generalklausel Datenverarbeitung[1]

Version 29.08.2017

Voraussetzung	Sachverhalt	Zur Erfüllung der Aufgaben erforderlich
	Erkenntnisse	./.
	Verfahren	./.
Richtung		./.
Folge	Zweckbind.	./.
	Mitteilungen	./.

Erläuterung	• Abgrenzung von nd-Mitteln: Datenerhebung beim Betroffenen offen unter Freiwilligkeitshinweis (§ 8 IV BVerfSchG) • Vertraulichkeitspflicht/Benachteiligungsverbot (§ 8b IV 2, V BVerfSchG)[2] • Ggf. Regelung bzgl. Trennungsprinzip, insbes. kein Ersuchen um Zwangsmaßnahmen oder Weisungen (§ 8 III BVerfSchG)[3] • Ggf. Regelung verbundener Begleiteingriffe von Erhebungen: o Beschränkung auf zulässig nutzbare Daten[4] (vgl. § 8d I 2 BVerfSchG); verbunden mit Begründungserläuterung, dass Erhebung gezielte Gewinnung ist (wenn beim Erhebungsvorgang weitere Informationen anfallen, steht dies der Erhebungszulässigkeit also nicht entgegen). o Angaben zur Bezeichnung des Interessegegenstandes (§ 8 I 2 BVerfSchG) • Ggf. Bekräftigung Erforderlichkeit / Verhältnismäßigkeit ieS (§ 8 I 3, V BVerfSchG)

[1] Begriff gem. BDSG nF (bisher: *Umgang* mit pbD)
[2] Die Regelung verfolgt keinen auf spezielle Befugnisse limitierten Zweck und sollte folglich querschnittsmäßig gelten, somit systematisch bereits in der allgemeinen Erhebungsnorm aufgenommen werden.
[3] Die Regelung ist sachlich überflüssig (nach dem Vorbehalt des Gesetzes bestehen ohnehin keine ungeschriebenen Befugnisse und nach allgemeinem Amtshilferecht richtet sich die Maßnahmezulässigkeit nach dem Recht der ersuchenden Behörde [§ 7 Abs. 1 VwVfg]). Sie besitzt aber Symbolgehalt. Gesetzesbefehle sollten jedoch auf Regelungsinhalte beschränkt werden, Erläuterungen ohne eigenen Regulierungsgehalt sollten vorzugsweise in der Gesetzesbegründung erfolgen. Wenn die Regelung gleichwohl in das Gesetz aufgenommen werden soll, erschiene § 2 I BVerfSchG passender.
[4] Der funktionale Bezug der Erhebung auf nachfolgende Nutzung und die resultierende Erforderlichkeitsbegrenzung bereits der Erhebung erscheinen zwar banal, angesichts der Rspr. des BVerfG (E 130, 151 / Rn. 185) könnte eine gesetzliche Regelung gleichwohl opportun sein. Allerdings sind speziell bei Maßnahmen zur Lageaufklärung Missverständnisse zur genauen Bedeutung einer solchen Regelung denkbar, weshalb vorzugswürdig erscheinen könnte, lediglich zu speziellen Befugnissen entsprechende Klarstellung aufzunehmen (so auch die Rspr. des BVerfG).

Regelungsbeispiel:

§ A Allgemeine Befugnisse

(1)[5] Die Verfassungsschutzbehörde darf die zur Erfüllung ihrer Aufgaben erforderlichen[6] personenbezogenen Daten[7] verarbeiten, soweit nicht die anzuwendenden Bestimmungen des …datenschutzgesetzes oder besondere Regelungen in diesem Gesetz entgegenstehen.

(2) Ein Ersuchen um Übermittlung personenbezogener Daten darf nur diejenigen personenbezogenen Daten enthalten, die für die Erteilung der Auskunft unerlässlich sind. Schutzwürdige Interessen des Betroffenen dürfen nur in unvermeidbarem Umfang beeinträchtigt werden.

(3)[8] Erhebt die Verfassungsschutzbehörde personenbezogene Daten beim Betroffenen mit seiner Kenntnis, so ist der Erhebungszweck anzugeben. Der Betroffene ist auf die Freiwilligkeit seiner Angaben hinzuweisen.

(4)[9] Erhebt die Verfassungsschutzbehörde Daten bei einem Dritten mit seiner Kenntnis, kann sie den Dritten zur Vertraulichkeit verpflichten, wenn der Zweck der Aufklärung dadurch gefährdet werden kann, dass der Betroffene oder Dritte von der Erhebung oder bei der Erhebung übermittelten Daten Kenntnis erhalten. Die Verpflichtung ist gegenüber nicht-öffentlichen[10] Stellen mit dem Hinweis zu verbinden, dass die Erhebung keinen Verdacht begründet, dass der Betroffene sich rechtswidrig verhalten hat. Der Verpflichtete darf an die Datenerhebung in Geschäftsverbindungen oder im Rechtsverkehr keine dem Betroffenen nachteiligen Folgen knüpfen[11].

(5) Von mehreren geeigneten Maßnahmen hat die Verfassungsschutzbehörde diejenige zu wählen, die den Betroffenen voraussichtlich am wenigsten beeinträchtigt. [Eine Maßnahme ist nicht geeignet, wenn mit ihr ein Mehraufwand verbunden ist, der erkennbar außer Verhältnis zur minderen Beeinträchtigung des Betroffenen steht.[12]] Eine Maßnahme darf keinen Nachteil herbeiführen, der erkennbar außer Verhältnis zu dem beabsichtigten Erfolg steht.

---

[5] § 8 I 1 BVerfSchG

[6] Zur Erhebung von Daten zu einer bestimmten Person kann eine „unscharfe" Anfrage erforderlich sein, wenn nach den vorhandenen Informationen eine zielgenauere Erhebung nicht möglich ist. Bsp.: phonetische oder unvollständige Kenntnis von Identifizierungsdaten; Kenntnis von Aufenthalt (zu bestimmter Zeit an bestimmtem Ort) der noch nicht identifizierten Zielperson - hier kann die Erhebung aller Personen, die den Suchkriterien entsprechen (z.B. „Funkzellen-Auskunft"), zur näheren Personenabklärung erforderlich sein.

[7] Regelung zu anderen (nicht-personenbezogenen) Informationen verzichtbar, da insoweit kein Eingriff, mithin kein Vorbehalt des Gesetzes - wäre in einer Gesetzesbegründung mit aufzunehmen.

[8] § 8 IV BVerfSchG

[9] § 8b IV 2, V BVerfSchG analog

[10] Im amtlichen Verkehr zwischen Behörden erscheint dies für den Schutzzweck nicht erforderlich

[11] Damit sind auch Verdachtsmeldungen aus Anlass der Datenerhebung der Verfassungsschutzbehörde, insbesondere Meldungen nach § 43 GWG, ausgeschlossen. Dies wäre jedenfalls in einer Gesetzesbegründung zu verdeutlichen, eventuell auch klarstellend im Gesetz selbst aufzunehmen.

[12] Bei Eingriffsakten ist nicht nur die Grundrechtsseite u.U. mehrpolig, auch Gemeinwohlbelange können mehrpolig kollateral betroffen sein. Bei der Würdigung des Übermaßverbots sind Gemeinwohlbelange gegen Individualbelange umfassend abzuwägen. Zu den einzubeziehenden Gemeinwohlbelangen zählen auch die Verwaltungsaufwände. Allerdings ist die Verwaltung insoweit betroffenenfreundlich erst bei Evidenz der Grenznutzendisproportionalität davon befreit, den für die Zweckverfolgung nicht erforderlichen Zusatzaufwand zu betreiben.

2 Allgemeine Regelungen zu nd-Mitteln

Version 29.08.2017

Voraussetzungen	Sachverhalt	Positiv: • Gefahrenlage (§ X Abs. 3) • Bei qualifizierten nd-Mitteln qualifizierte Gefahrenlage (§ X Abs. 3 Satz 3) • Besonders sensible Maßnahmen gesondert speziell geregelt (§ X Abs. 2) Negativ: • Befugnisgehalt zum Individualrechtseingriff auf Datenerhebung beschränkt (§ X+1 Abs. 1 S. 2) • Dieser Eingriff beschränkt durch Kernbereichsschutz (§ X+1 Abs. 2 Nr. 1) • Erlaubnisgehalt zum Universalrechtseingriff schließt nicht Rechtsprechungs- und Parlamentsfunktionen (§ X+1 Abs. 1 S. 1) und nicht bestimmte Vertrauensverhältnisse/Zeugnisverweigerungsrechte (§ X+1 Abs. 2 Nr. 2) ein • Allg. Übermaßverbot (entsprechend auch für Beeinträchtigung rechtlich geschützter öffentlicher Interessen / Universalrechtsgüterschutz), § X+1 Abs. 1 S. 3, Abs. 5 und 6, aber kein abschließender Katalog übertretbarer Normen
	Erkenntnisse	• Gefahrenlage durch Verdachtsfall-BO (nicht beim Prüffall), § X Abs. 3 S. 2
	Verfahren	• In DV zu regeln (mit Zustimmung Ministerium und Unterrichtung PKGr), § X+7 Abs. 1 S. 1 • Besondere Regelungen zum Schutz Kernbereich / bestimmter Zeugnisverweigerungsrechte (§ X Abs. 3), mit spezieller Regelung für Aufzeichnungen und besonderen Maßgaben insbes. zu WRÜ/ODS und spezifischen Verfahrenssicherungen für Kernbereichsschutz (Abs. 4) • Besonders sensible Maßnahmen (Eingriff in Art. 10, 13 GG oder informationstechnische Systeme) mit gesonderten Anordnungs-/Kontroll-/Verfahrensregelungen (§ X+7 bis X+10)
Richtung		• Grundsätzlich Verdachtsfindungseingriff durch Lageerforschung (keine Richtungsindividualisierung), § X Abs. 4 Satz 2 • Qualifizierte nd-Mittel auf „Gefährder“ und durch spezifische individuelle Nähe Verstrickte (§ X Abs. 4) beschränkt • Besonders sensible Maßnahmen gesondert speziell geregelt (§ X Abs. 2)
Folgen	Zweckbind.	./. (Besonders sensible Maßnahmen gesondert geregelt, § X+4 bis X+6; iÜ gilt allgemein bei Übermittlungen an Nicht-ND zweckbezogene Übermittlungsschwellen und Empfängerbindung an Übermittlungszweck, § 19 I BVerfSchG)
	Mitteilungen	• Bei qualifizierten nd-Mitteln (mit Ausnahme-/Absehensregelung), § X+10

Erläuterung	• Kein abschließender Katalog der nd-Mittel (§ X Abs. 1 S. 2: „insbes.“), aber über PKGr-Verfahren (§ X Abs. 1 Satz 3) gewährleistet, dass keine untergesetzliche Maßnahmeergänzung im Bereich des Vorbehalts des Gesetzes • Querschnittsregelungen sind zur Vermeidung von Wiederholungen in den besonderen Befugnisnormen „vor die Klammer gezogen“. Zur analytischen Grundlage wird auf die Auswertung der jeweiligen Befugnis verwiesen.

Regelungsbeispiel:

§ X Nachrichtendienstliche Mittel

(1) Die Verfassungsschutzbehörde darf Methoden, Gegenstände und Instrumente zur heimlichen Informationsbeschaffung (nachrichtendienstliche Mittel) zur Aufklärung von Bestrebungen und Tätigkeiten anwenden, wenn hinreichende Anhaltspunkte bestehen, dass die Bestrebungen oder Tätigkeiten ziel- und zweckgerichtet gegen die in § 3 Absatz 1 oder Satz 1 Nummer 2 genannten Schutzgüter gerichtet sind[1]. Nachrichtendienstliche Mittel sind insbesondere

1. *Legenden, insbesondere fingierte biographische, berufliche oder gewerbliche Angaben, und Beschaffung, Erstellung und Verwendung von Tarnpapieren und Tarnkennzeichen,*
2. *Personen, die der Verfassungsschutzbehörde logistische oder sonstige Hilfe leisten (Gewährspersonen),*
3. *Personen, die in Einzelfällen oder gelegentlich wegen ihrer Kontakte zu einem Beobachtungsfeld Hinweise geben (Informanten),*
4. *Informationserhebungen im Internet unter Ausnutzung schutzwürdigen Vertrauens Betroffener,*
5. *Ermittlungen, ohne deren tatsächlichen Zweck anzugeben (verdeckte Ermittlungen),*
6. *Observationen,*
7. *für Observationszwecke bestimmte technische Mittel (technische Observation), insbesondere zur Feststellung des Aufenthaltsortes und zum heimlichen Aufzeichnen des nicht öffentlich gesprochenen Wortes oder von Bildern,*
8. *elektronische Signalaufklärungen, einschließlich der Ermittlung des Standortes eines aktiv geschalteten Mobilfunkendgerätes oder zur Ermittlung der Geräte- oder Kartennummer[2],*
9. *vorübergehende heimliche Inbesitznahmen von Sachen zur Datenerhebung[3].*

---

[1] Die Regelung erfolgt komplementär zu § 4 Absatz 1 Satz 3 und schließt den Einsatz von nd-Mitteln bei bloßen Prüffällen aus. Zulässig ist der Einsatz erst bei Beobachtungsobjekten (einschließlich - also ab - Verdachtsfall). Der Begriff „*hinreichende*“ Anhaltspunkte umschreibt dabei eine gegenüber - sehr niederschwelligen - *tatsächlichen* Anhaltspunkten (die bereits zum Prüffall erforderlich sind) zum Verdacht verdichtete Erkenntnislage. Bei einer umfassenderen Gesetzesnovelle, solle erwogen werden, den Prozess der BO-Festlegung gesondert gesetzlich zu regeln (vgl. §§ 6 ff NVerfSchG; der dortigen Unterscheidung Anfangsverdacht/Verdacht korrespondieren hier tatsächliche/hinreichende Anhaltspunkte. Begriff „hinreichend“ bezeichnet eine Schwelle für anknüpfende Folgen, diese in den Verdachtsanforderungen abwägend.

[2] Eine spezielle Regelung zum IMSI-Catchereinsatz ist nicht erforderlich, da insoweit keine besonderen Voraussetzungen gelten sollen. Es handelt sich lediglich um ein bestimmtes Mittel elektronischer Signalaufklärung, das insbesondere nicht mit einem Eingriff in Art. 10 GG verbunden ist (BVerfG, Beschluss vom 22. August 2006 - 2 BvR 1345/03 - / Rn. 57).

[3] Hierunter fällt vornehmlich die Inbesitznahme von Datenträgern (konventionelle Unterlagen ebenso wie elektronische Speicherung) zu deren Auslesung, ferner aber auch Sachen, die auf Spuren (etwa Fingerabdrücke) untersucht werden. Die Regelung ist zugleich eine besondere Befugnis im Sinne des § x+1 Abs. 1 Satz 2, die den verbundenen Eingriff in das Besitzrecht des Besitzers rechtfertigt. Der Spezialfall Post ist ergänzend in § X+3 speziell geregelt, worauf Absatz 2 Nr. 2 verweist.

Die Verfassungsschutzbehörde hat die nachrichtendienstlichen Mittel in einer Dienstvorschrift abschließend zu benennen. Die Dienstvorschrift bedarf der Zustimmung des …ministeriums des Innern, das das Parlamentarische Kontrollgremium unterrichtet.

(2) Die Verfassungsschutzbehörde darf

1. *verdeckte Ermittlungen (Absatz 1 Nummer 5) durch planmäßigen dauerhaften zur Informationsbeschaffung eingesetzte Personen,*
   a) *deren Einsatz für die Verfassungsschutzbehörde nicht bekannt ist (Vertrauensleute),*
   b) *die als eigene Mitarbeiter unter einer auf Dauer angelegten Legende eingesetzt werden (Verdeckte Mitarbeiter)*

   nur nach Maßgabe des § X+2,
2. *technische Observationen und elektronische Signalaufklärung (Absatz 1 Nummer 7 und 8) unter Eingriff in Artikel 10, 13 GG oder informationstechnische Systeme und Maßnahmen nach Absatz 1 Nummer 9 unter Eingriff in Artikel 10 GG nur nach Maßgabe der §§ X+3 bis X+5*

durchführen.

(3) Die Verfassungsschutzbehörde darf personenbezogene Daten mit nachrichtendienstlichen Mitteln nur erheben, wenn Tatsachen die Annahme rechtfertigen[4] (tatsächliche Anhaltspunkte), dass

1. *auf diese Weise Erkenntnisse über*
   a) *Bestrebungen oder Tätigkeiten nach § 3 Absatz 1 oder*
   b) *die zu deren Aufklärung erforderlichen Quellen (Absatz 1 Nummer 2 und 3, Absatz 2 Nummer 1 Buchstabe a)*

   gewonnen werden können oder
2. *dies zum Schutz der Mitarbeiter, Einrichtungen, Gegenstände und nachrichtendienstlichen Verbindungen der Verfassungsschutzbehörde gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten[5] erforderlich ist.*

Ein dauerhafter Einsatz von verdeckten Ermittlungen nach Absatz 2 Nummer 1, Observationen, auch technischen, und elektronischer Signalaufklärung (Absatz 1 Satz 1

[4] Die folgenden Tatbestandsvoraussetzungen beschreiben die Gefahrerforschung einer Gefahrenlage (risikoindizierender Sachverhalt / allgemein bestehende Gefahr) zur Lagebewertung und zur Entdeckung konkreter Gefahren

[5] Entspricht § 9 I 1 Nr. 2 BVerfSchG und geht insoweit über Nummer 1 Buchstabe a (iVm § 3 I Nr. 2 BVerfSchG) hinaus, als nicht vorausgesetzt wird, dass eine fremde Macht tätig ist („geheimdienstliche Tätigkeit“ umschreibt die Handlungsmethodik, die unabhängig von einem behördlichen Aufgabenträger auch von Bestrebungen oder anderen Angreifern genutzt werden kann).

Nummern 6 bis 8) ist zur Aufklärung von Bestrebungen nur zulässig, wenn diese erhebliche Bedeutung haben[6].

(4) Observationen, auch technische, und Signalaufklärung (Absatz 1 Nummer 6 bis 8[7]) dürfen sich nur gegen Personen richten, zu denen tatsächliche Anhaltspunkte dafür vorliegen, dass sie

1. *an den Bestrebungen oder Tätigkeiten nach Absatz 3 Nummer 1 Buchstabe a durch*
   a) *eigenes Verhalten oder*
   b) *eigene Sachen, die für die Bestrebungen oder Tätigkeiten genutzt werden,*

   beteiligt sind,
2. *die in Absatz 3 Nummer 2 bezeichneten Schutzgüter entsprechend Nummer 1 Buchstabe a oder b konkretisiert[8] gefährden oder*
3. *im Zusammenhang mit einer Person nach Nummer 1 oder 2 stehen und durch die Maßnahme Erkenntnisse, die nicht gleichermaßen nach Nummer 1 oder 2 zu gewinnen sind, über die Bestrebungen, Tätigkeiten oder Gefährdungen gewonnen werden können.*

Die Maßnahme darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden. Soweit in §§ X+3 bis X+5 keine besonderen Regelungen getroffen sind, dürfen andere Maßnahmen unter den Voraussetzungen des Absatzes 3 auch durchgeführt werden, um tatsächliche Anhaltspunkte zu solchen Personen zu gewinnen. Ein systematischer Einsatz nachrichtendienstlicher Mittel[9] zur Gewinnung von Daten zu einer Person (Zielperson) ist nur zu Personen nach Satz 1 zulässig. Ist anzunehmen, dass der Betroffene keine Kenntnis über seine spezifische individuelle Nähe zu der aufzuklärenden Gefahr (Satz 1) hat, müssen hinreichende Anhaltspunkte für seine Verstrickung bestehen[10]. Die Überprüfung der Zuverlässigkeit einer Quelle (Absatz 3 Nummer 1 Buchstabe b) bleibt unberührt.

---

[6] Übernahme aus § 9a Abs. 1 Satz 2 BVerfSchG. An dortige Gesetzesmaterialien angelehnt könnte „erhebliche Bedeutung“ in § 4 BVerfSchG legaldefiniert werden (BT-Drs.: 18/4654, S. 26: „Gesamtwürdigung der Gefährlichkeit der Bestrebung – insbesondere im Hinblick auf Größe, Einfluss und Abschottung“, wobei im Ergebnis lediglich BO mit geringer Bedeutung, d.h. unterster Priorisierung ausgeschieden werden, für deren Aufklärung die Ressourcen besonderer nd-Mittel fehlgesteuert wären). Die erhebliche Bedeutung der mit einem BO begründeten Gefahrenlage korrespondiert wertend einer Strafverfolgungsbeschränkung auf Delikte von erheblicher Bedeutung, die das BVerfG dort als Voraussetzung bspw. einer technischen Observation mit GPS-Sender annimmt (BVerfGE 141, 220 / Rn. 107).

[7] Maßnahmetypik ist individualisiert, Maßnahmerichtung gem. individueller Gefahrenverantwortung.

[8] Der Begriff „konkretisiert“ referenziert auf die Rspr. des BVerfG, das damit eine individuelle Gefahr im Sinne einer persönlichen Handlungsdispositivität bezeichnet (individuelles Verhalten lässt auf künftige Störungshandlung schließen, ohne dass die Art der Durchführung bereits abschätzbar wäre; zu dieser Form einer individuell konkretisierten Gefahr als Maßnahmeschwelle: BVerfGE 141, 220 / Rn. 164).

[9] Also insgesamt, nicht nur die in Satz 1 bereits speziell geregelten Mittel.

[10] Gefahrenabwehr ist schuldunabhängig. Bei undolos verstrickten Personen ist die Verantwortlichkeit aber geringer zu gewichten. In der Verhältnismäßigkeitsabwägung muss dies mit einer höheren Erkenntnisdichte (*hinreichende* Anhaltspunkte) kompensiert werden.

§ X+1 Schranken nachrichtendienstlicher Mittel

(1) Beim Einsatz nachrichtendienstlicher Mittel sind Schutznormen der Rechtspflege[11] und der parlamentarischen Kontrolle zu beachten. In Individualrechte darf durch nachrichtendienstliche Mittel nur nach Maßgabe besonderer Befugnisse eingegriffen werden. Der Einsatz nachrichtendienstlicher Mittel ist unzulässig, wenn die Erforschung des Sachverhalts auf andere, den Betroffenen oder ein rechtlich geschütztes öffentliche Interesse weniger beeinträchtigende Weise möglich ist. Eine geringere Beeinträchtigung ist in der Regel anzunehmen, wenn die Information aus allgemein zugänglichen Quellen oder durch eine Auskunft nach § 18 Absatz 3 [BVerfSchG] gewonnen werden kann.

(2) Eine Maßnahme ist unzulässig, soweit

1. *tatsächliche Anhaltspunkte dafür vorliegen, dass durch sie allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung gewonnen werden würden, oder*
2. *Informationen bei einer in § 53 Absatz 1 Satz 1 Nummer 1, 2, 3 oder Nummer 4 der Strafprozessordnung genannten Person, im Falle dessen Nummer 3 beschränkt auf Rechtsanwälte oder Kammerrechtsbeistände, oder deren Berufshelfer (§ 53a der Strafprozessordnung) nicht zur Aufklärung von Bestrebungen oder Tätigkeiten dieser Personen erhoben werden und die Maßnahme voraussichtlich Erkenntnisse erbringen würde, über die diese Person das Zeugnis verweigern dürfte.*

Werden solche Erkenntnisse bei einer Maßnahme gewonnen, dürfen sie nicht genutzt werden. Aufzeichnungen solcher Erkenntnisse sind zu löschen. Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist in Fällen, in denen Mitteilung nach § X+10 erfolgt, sechs Monate nach der Mitteilung oder dem abschließenden Absehen von der Mitteilung, im Übrigen am Ende des Kalenderjahres, das der Protokollierung folgt, zu löschen.

(3) Ergeben sich bei der Maßnahme während der Durchführung tatsächliche Anhaltspunkte dafür, dass Inhalte des Kernbereichs privater Lebensgestaltung erfasst werden, ist die Maßnahme zu unterbrechen, sobald dies ohne Gefährdung eingesetzter Personen möglich ist und solange die Anhaltspunkte bestehen. Bei technischer Observation und elektronischer Signalaufklärung (§ X Absatz 1 Nummern 7 und 8, § X Absatz 2 Nummer 2) dürfen Aufzeichnungen fortgesetzt werden, wenn Zweifel am Vorliegen solcher Inhalte bestehen. Diese Aufzeichnungen sind unverzüglich der Kommission [nach § 15 des Artikel 10-Gesetzes] vorzulegen. Sie dürfen nur mit ihrer

[11] Das Schutzgut ist vom Rechtsverkehr zu entscheiden. Die Regelung dient der Funktionssicherung der Gewaltenteilung. Verboten ist mithin Meineid, aber nicht Urkundsfälschung.

Zustimmung genutzt werden. Die Kommission entscheidet durch ein Mitglied (Bereitschaftsmitglied), das die Befähigung zum Richteramt besitzen muss. Die Bereitschaftszuständigkeit wird in der Geschäftsordnung der Kommission näher geregelt. Das Bereitschaftsmitglied berichtet der Kommission in deren nächster Sitzung. Entscheidet das Bereitschaftsmitglied oder die Kommission, dass die weitere Verarbeitung unzulässig ist, gelten Absatz 2 Sätze 2 bis 6.

(4) Bei Gefahr im Verzug können Aufzeichnungen nach Absatz 3 Satz 2 unter Aufsicht eines Bediensteten, der die Befähigung zum Richteramt hat, gesichtet werden[12]. Der Bedienstete entscheidet im Benehmen mit dem Beauftragten für den Datenschutz (§ 4f BDSG)[13] über eine vorläufige Nutzung.

(5) Die Beeinträchtigung rechtlich geschützter Interessen durch Anwendung eines nachrichtendienstlichen Mittels darf nicht erkennbar außer Verhältnis zur Bedeutung des aufzuklärenden Sachverhaltes stehen. Erfolgen Maßnahmen bei einer in § 53 Absatz 1 Satz 1 Nummer 3 bis 3b oder Nummer 5 der Strafprozessordnung genannten Person oder deren Berufshelfer (§ 53a der Strafprozessordnung) nicht zur Aufklärung von Bestrebungen oder Tätigkeiten dieser Personen, ist das öffentliche Interesse an den von dieser Person wahrgenommenen Aufgaben und das Interesses an der Geheimhaltung der dieser Person anvertrauten oder bekannt gewordenen Tatsachen besonders zu berücksichtigen. Für Rechtsanwälte oder Kammerrechtsbeistände bleiben Absätze 2 bis 4 unberührt.

(6) Eine Maßnahme ist unverzüglich zu beenden, wenn ihr Zweck erreicht ist oder sich Anhaltspunkte dafür ergeben, dass er nicht oder nicht auf diese Weise erreicht werden kann.

[12] Eine gesonderte Verschwiegenheitsregelung ist angesichts Absatz 3 Satz 4 überflüssig.
[13] Die Regelung nimmt auf das Amt, nicht eine Person Bezug, d.h. Vertretungsregelungen sind ohne weiteres anzuwenden.

§ X+6 Einsatzfreigabe und Protokollierung nachrichtendienstlicher Mitteln

(1) Die Zuständigkeit für die Einsatzfreigabe nachrichtendienstlicher Mittel ist in der Dienstvorschrift nach § X Absatz 1 Satz 2 zu regeln. Für Einsatzfreigaben der Mittel nach §§ X+3 bis X+5 Absatz 1, auch in Verbindung mit Absatz 5, (Anordnungen) gelten die nachfolgenden Absätze[14]*.*

(2) Anordnungen sind von der Behördenleitung der Verfassungsschutzbehörde oder ihrer Stellvertretung zu beantragen. Im Antrag sind anzugeben:

1. *die Person, gegen die sich die Maßnahme richtet, soweit möglich, mit Name und Anschrift,*
2. *Art, Umfang und Dauer der Maßnahme,*
3. *weitere in §§ X+3 bis X+5 Absatz 1 bestimmte Angaben,*
4. *der Sachverhalt sowie*
5. *eine Begründung.*

(3) Zuständig für die Anordnung ist das …ministerium des Innern. Die Anordnung ergeht schriftlich. In ihr sind Angaben entsprechend Absatz 2 aufzunehmen. Liegen die Voraussetzungen der Anordnung nicht mehr vor, sind die aufgrund der Anordnung ergriffenen Maßnahmen unverzüglich zu beenden. Die Beendigung ist dem …ministerium des Innern anzuzeigen.

(4) Das Bundesamt für Verfassungsschutz unterrichtet die jeweilige Landesbehörde für Verfassungsschutz über die in deren Bereich getroffenen Anordnungen. Die Landesbehörden für Verfassungsschutz teilen dem Bundesamt für Verfassungsschutz die in ihrem Bereich getroffenen Anordnungen mit.

(5) Bei Maßnahmen nach § X Absatz 1 Nummern 6 bis 9 oder § X Absatz 2 gegen Zielpersonen (§ X Absatz 4 Satz 4) ist die Durchführung mit Angaben entsprechend Absatz 2 Nummern 1 bis 3 zu protokollieren, bei Maßnahmen nach § X+4 zusätzlich mit Angaben zu den am informationstechnischen System vorgenommenen nicht nur flüchtigen Veränderungen[15]*.*

§ X+7, +8 Kontrolle [Regelungen entsprechen §§ 14, 15 G 10[16]*]*

---

[14] Dieser Anwendungsbereich für besondere Anordnungsverfahren folgt der Verfassungsentscheidung, besonderen Freiheitsschutz in speziellen („benannten“) Grundrechten auszuprägen: Das spezielle Anordnungsverfahren ist kongruent für Eingriffe in Art. 10 und 13 GG vorgesehen (wobei auf die Online-Datenerhebung Art. 13 GG entsprechend bezogen wird). Zu den unterschiedlichen Schlussfolgerungen in der AG aus dem Urteil des BVerfG zum BKAG siehe im Bericht Abschnitt 3.1.

[15] Die Regelung konkretisiert Anforderungen an die aktenmäßige Dokumentation des Verwaltungshandelns. Zugleich werden damit Anforderungen verfahrensmäßiger Kontrollsicherung erfüllt, die das BVerfG bei qualifizierten Überwachungsmaßnahmen als gesetzlich regelungsbedürftig ansieht (BVerfGE 141, 220, Rn. 141, 267). Da sich der Dokumentationszweck indes nicht auf Kontrollsicherung beschränkt, wird die Nutzung - anders als in § 82 Abs. 4 BKAG - nicht speziell beschränkt.

[16] Die „G 10-Kommission“ wird als „Kommission“ bezeichnet. Im Zusammenhang der § 15 VI 2 G 10 entsprechenden Regelung wäre für Maßnahmen nach §§ X+4 und X+5 (ODS/WRÜ) vorzusehen, dass nach Eilanordnung des BMI unverzüglich die Kommissionsentscheidung herbeizuführen ist (die Entscheidung im Sitzungsturnus genügt nicht den Anforderungen des Art. 13 Abs. 4 GG).

§ X+9 Weitere Verfahrensregelungen zu angeordneten nachrichtendienstlichen Mitteln

(1) Das …amt für Verfassungsschutz prüft unverzüglich und sodann in Abständen von höchstens sechs Monaten, ob die nach § X+3 bis § X+5 Absatz 1 erhobenen personenbezogenen Daten für ihre Aufgaben nach § 3 Absatz 1 [BVerfSchG] erforderlich sind. Eine Löschung nach § 12 Absatz 2 Satz 1 [BVerfSchG] erfolgt unter Aufsicht eines Bediensteten, der die Befähigung zum Richteramt hat. Die Löschung ist zu protokollieren. Die Protokolldaten dürfen ausschließlich zur Durchführung der Datenschutzkontrolle verwendet werden. Die Protokolldaten sind sechs Monate nach der Mitteilung nach § X+10, spätestens jedoch am Ende des Kalenderjahres, das dem Jahr der Protokollierung folgt, zu löschen. Die Löschung der Daten unterbleibt, soweit die Daten für eine Mitteilung nach § X+10 oder für eine gerichtliche Nachprüfung der Rechtmäßigkeit der Beschränkungsmaßnahme von Bedeutung sein können. In diesem Fall ist die Verarbeitung der Daten einzuschränken; sie dürfen nur zu diesen Zwecken verwendet werden.

(2) Die verbleibenden Daten sind zu kennzeichnen[17]. Die Behördenleitung oder ihre Stellvertretung kann anordnen, dass bei der Übermittlung[18] auf die Kennzeichnung verzichtet wird, wenn dies unerlässlich ist, um die Geheimhaltung einer Beschränkungsmaßnahme nicht zu gefährden, und die Kommission zugestimmt hat. Bei Gefahr im Verzuge kann die Anordnung bereits vor der Zustimmung getroffen werden. Wird die Zustimmung versagt, ist die Kennzeichnung durch den Übermittlungsempfänger unverzüglich nachzuholen; die übermittelnde Behörde hat ihn hiervon zu unterrichten.

(3) Nach einer Übermittlung ist die Kennzeichnung durch den Empfänger aufrechtzuerhalten. Er prüft unverzüglich und sodann in Abständen von höchstens sechs Monaten, ob die übermittelten Daten für die Zwecke, zu deren Erfüllung sie ihm übermittelt worden sind, erforderlich sind. Absatz 1 Satz 2 und 3 gilt entsprechend. Der Empfänger unterrichtet die übermittelnde Stelle unverzüglich über die erfolgte Löschung.

[17] In Begründung klarstellen, dass die Regelungen nur für die mit der Maßnahme gewonnen (Roh-)Daten gelten, nicht für Erkenntnisse, die unter Einbezug weiterer Daten/Erkenntnisse gewonnen werden (keine Fernwirkung der gewonnen Ansätze auf angereicherte Analyseprodukte).

[18] Ein Anfragedatensatz bei einem Erhebungsersuchen ist in diesem Sinne keine Übermittlung (für Empfängeraufgaben) und erfordert danach von vornherein keine Kennzeichnung.

§ X+10 Mitteilung an Betroffene

(1) Zielpersonen von Maßnahmen nach [§ X Absatz 1 Satz 2 Nummer 7 und][19] §§ X+3 bis X+5 Absatz 1 ist mitzuteilen, dass zu ihnen Daten mit nachrichtendienstlichen Mitteln[20] erhoben worden sind. Die Mitteilung erfolgt, sobald zur Zielperson keine nachrichtendienstlichen Mittel mehr eingesetzt werden dürfen. Wurden personenbezogene Daten übermittelt, erfolgt die Mitteilung im Benehmen mit dem Empfänger. Die Mitteilung unterbleibt entsprechend § 15 Absatz 2 Satz 1 Nummer 1 bis 3[21] [BVerfSchG].

(2) Das weitere Vorliegen der Voraussetzungen des Absatzes 1 Satz 4 ist erstmals nach höchstens zwölf Monaten und im weiteren nach festgesetzten Fristen, die die Löschungsprüffristen nicht übersteigen dürfen[22], zu überprüfen. Von einer Mitteilung kann nach fünf Jahren abgesehen werden, wenn die Voraussetzungen weiter vorliegen [und ihr Wegfall nicht absehbar ist]. Die Entscheidung nach Satz 2 trifft die Behördenleitung oder ein von ihr besonders beauftragter Mitarbeiter.

(3) Erfolgt bei Maßnahmen nach § X+3 bis X+5 Absatz 1 eine Mitteilung nicht binnen zwölf Monaten bedarf die weitere Zurückstellung der Zustimmung der Kommission. Sie bestimmt die Dauer einer weiteren Zurückstellung. Von einer Mitteilung kann nach fünf Jahren abgesehen werden, wenn die Kommission einstimmig festgestellt hat, dass

1. *die Voraussetzungen nach Absatz 1 Satz 4 noch vorliegen und*
2. *eine Mitteilung mit an Sicherheit grenzender Wahrscheinlichkeit[23] auch in Zukunft nicht erfolgen würde. Liegen die Voraussetzungen für eine Löschung der erhobenen Daten sowohl bei der Verfassungsschutzbehörde als auch bei den Empfängern dieser Daten vor, genügt, dass auf absehbare Zukunft keine Mitteilung erfolgen würde.*

---

[19] Die Erweiterung über Maßnahmen nach X+3 bis X+5 (mit den bisherigen Mitteilungspflichten nach § 12 G 10) hinaus soll Mitteilungspflichten nach § 9 Abs. 3 BVerfSchG und entsprechenden landesrechtlichen Vorschriften aufgreifen. Da dort einschränkende Maßgaben enthalten sind, ist der allgemeine Bezug auf § X Absatz 1 Satz 2 Nummer 7 jedoch eventuell überschießend, bedürfte jedenfalls noch näherer Prüfung, insbesondere auf eine etwaigen Beschränkung auf qualifizierte Fälle, die den Sachverhalt auch zur Wertungskonsistenz deutlich über Maßnahmen nach § X Absatz 1 Satz 2 Nummer 6 hinaus heben. Entfiele die Maßnahme ganz, wäre infolge auch Absatz 2 als gegenstandslos zu streichen.

[20] Keine Angabe des Mittels

[21] Nr. 2, 2. Alt. (Ausforschungsgefahr) ist nicht einschlägig, da Initiativmitteilung erfolgt. Die Überprüfungspflicht begründet keine Befugnis zu grundrechtseingriffsvertiefenden Maßnahmen; wenn eine zustellungsfähige Anschrift nicht vorliegt, wird endgültig von einer Mitteilung abgesehen.

[22] Die Synchronisierung mit der Löschungsprüfung reduziert die verbundenen Verwaltungsaufwände bei Gewährleistung fortdauernder Prüfroutinen. Den Löschungsprüffristen liegen Einschätzungen zur potenziellen Relevanz von Zeitablauf für die Beurteilung des Sachverhalts zugrunde, die hier ebenso einen äußeren zeitlichen Rahmen sachgerecht vorgeben.

[23] Die Regelung folgt § 101 StPO (dazu: BVerfG, NJW 2012, 833, Rz. 241f) und weicht damit aber von § 12 I 5 Nr. 3 G 10 ab. Dies birgt Risiken, da das BVerfG im BKAG-Urteil ebenfalls kumulativ Löschung voraussetzt, BVerfGE 141, 220, Rn. 262. Dabei geht das Gericht aber davon aus, dass für das Absehen von Mitteilung bereits genügt, wenn „*aller Wahrscheinlichkeit nach* auf Dauer“ keine Mitteilung erfolgt (BVerfG, NJW 2012, 833, Rz. 242). Wenn dies hingegen praktisch mit *Sicherheit* prognostizierbar ist, sind verbundene Aufwände und erwartbarer Nutzen unter Einbezug des mit Zeitablauf zunehmend ausdünnenden Rechtsschutzinteresses gesondert abzuwägen. Möglicherweise ist gleichwohl aus pragmatischen Gründen an § 12 Abs. 1 G 10 festzuhalten, da dies verfassungsrechtliche Risiken vermeidet und die Kommission voraussichtlich so oder so extrem restriktiv beim endgültigen Absehen verfahren wird.

3	Vertrauensleute, Verdeckte Mitarbeiter

Version 29.08.2017

Erläuterung	Die Regelung übernimmt die erst in 2015 nach einem sensiblen politischen Meinungsbildungsprozess in das BVerfSchG eingefügten §§ 9a, b vollinhaltlich. § 9a Abs. 1 S. 2 ist dabei bereits systematisch vor die Klammer gezogen in § X Abs. 3 S. 3 getroffen, braucht also in § X+2 nicht wiederholt zu werden. Im Übrigen wird auf eine systematische Differenzierung in 2 Paragraphen verzichtet.

Regelungsbeispiel:

§ X+2 Vertrauensleute, Verdeckte Mitarbeiter[1]

(1) Über die Verpflichtung von Vertrauensleuten (§ X Absatz 2 Nummer 1 Buchstabe a) entscheidet der Behördenleiter oder sein Vertreter. Als Vertrauensleute dürfen Personen nicht angeworben und eingesetzt werden, die

1. *nicht voll geschäftsfähig, insbesondere minderjährig sind,*
2. *von den Geld- oder Sachzuwendungen für die Tätigkeit auf Dauer als alleinige Lebensgrundlage abhängen würden,*
3. *an einem Aussteigerprogramm teilnehmen,*
4. *Mitglied des Europäischen Parlaments, des Deutschen Bundestages, eines Landesparlaments oder Mitarbeiter eines solchen Mitglieds sind oder*
5. *im Bundeszentralregister mit einer Verurteilung wegen eines Verbrechens oder zu einer Freiheitsstrafe, deren Vollstreckung nicht zur Bewährung ausgesetzt worden ist, eingetragen sind.*

Der Behördenleiter kann eine Ausnahme von Nummer 5 zulassen, wenn die Verurteilung nicht als Täter eines Totschlags (§§ 212, 213 des Strafgesetzbuches) oder einer allein mit lebenslanger Haft bedrohten Straftat erfolgt ist und der Einsatz zur Aufklärung von Bestrebungen, die auf die Begehung von in § 3 Absatz 1 des Artikel 10-Gesetzes bezeichneten Straftaten gerichtet sind, unerlässlich ist. Im Falle einer Ausnahme nach Satz 3 ist der Einsatz nach höchstens sechs Monaten zu beenden, wenn er zur Erforschung der in Satz 3 genannten Bestrebungen nicht zureichend gewichtig beigetragen hat. Auch im Weiteren ist die Qualität der gelieferten Informationen fortlaufend zu bewerten.

[1] verfassungsschutzinterne Bezeichnung: UCA

(2) Vertrauensleute dürfen weder zur Gründung von Bestrebungen nach § 3 Absatz 1 Nummer 1, 3 oder 4 noch zur steuernden Einflussnahme auf derartige Bestrebungen eingesetzt werden. Sie dürfen in solchen Personenzusammenschlüssen oder für solche Personenzusammenschlüsse, einschließlich strafbaren Vereinigungen, tätig werden, um deren Bestrebungen aufzuklären. Im Übrigen ist im Einsatz eine Beteiligung an Bestrebungen zulässig, wenn sie

1. *nicht in Individualrechte eingreift,*
2. *von den an den Bestrebungen Beteiligten derart erwartet wird, dass sie zur Gewinnung und Sicherung der Informationszugänge unumgänglich ist und*
3. *nicht außer Verhältnis zur Bedeutung des aufzuklärenden Sachverhalts steht.*

Sofern zureichende tatsächliche Anhaltspunkte dafür bestehen, dass Vertrauensleute rechtswidrig einen Straftatbestand von erheblicher Bedeutung verwirklicht haben, soll der Einsatz unverzüglich beendet und die Strafverfolgungsbehörde unterrichtet werden. Über Ausnahmen nach Satz 4 entscheidet der Behördenleiter oder sein Vertreter.

[(3)[2] Die Staatsanwaltschaft kann von der Verfolgung von im Einsatz begangenen Vergehen absehen oder eine bereits erhobene Klage in jeder Lage des Verfahrens zurücknehmen und das Verfahren einstellen, wenn

1. *der Einsatz zur Aufklärung von Bestrebungen erfolgte, die auf die Begehung von in § 3 Absatz 1 des Artikel 10-Gesetzes bezeichneten Straftaten gerichtet sind, und*
2. *die Tat von an den Bestrebungen Beteiligten derart erwartet wurde, dass sie zur Gewinnung und Sicherung der Informationszugänge unumgänglich war.*

Dabei ist das Verhältnis der Bedeutung der Aufklärung der Bestrebungen zur Schwere der begangenen Straftat und Schuld des Täters zu berücksichtigen. Ein Absehen von der Verfolgung ist ausgeschlossen, wenn eine höhere Strafe als ein Jahr Freiheitsstrafe zu erwarten ist. Ein Absehen von der Verfolgung ist darüber hinaus stets ausgeschlossen, wenn zu erwarten ist, dass die Strafe nicht zur Bewährung ausgesetzt werden würde. Die Sätze 1 bis 4 gelten auch in Fällen der Landesbehörden für Verfassungsschutz.]

(4) Die Bundesregierung trägt dem Parlamentarischen Kontrollgremium mindestens einmal im Jahr einen Lagebericht zum Einsatz von Vertrauensleuten vor.

(5) Die Absätze 2 und 3 sind entsprechend auf den Einsatz von Verdeckten Mitarbeitern (§ X Absatz 2 Nummer 1 Buchstabe b) anzuwenden.

---

[2] Regelungsvorschlag nur für den Bund (Strafprozessrecht - vgl. § 9a III BVerfSchG) - hier im Zusammenhang dargestellt wie es der derzeitigen Regelungstechnik im Bund entspricht.

4 Eingriffe in Art 10 GG

Version 29.08.2017

Voraussetzungen	Sachverhalt	• Verkehrsdaten: Aufklärung von Bestrebungen von erheblicher Bedeutung[1] • Vorsorgedaten: Synchron mit Inhaltsüberwachung • Inhaltsüberwachung: § 3 I G 10 (schwere Gefahren) • Erweiterte Quellen-TKÜ (inkl. „ruhenden“ Verkehren): § 3 I G 10
	Erkenntnisse	./.
	Verfahren	• Wie G 10 (zusammengefasst in §§ X+6 ff geregelt)
Richtung		• Wie G 10
Folgen	Zweckbind.	• Offener als G 10, aber an Nicht-ND weiter aufgabenadäquat beschränkt; spezielle Regelung bei dringendem Verdacht
	Mitteilungen	• Ähnlich G 10 (§ X+10)

Erläuterung	• Im Anwendungsbereich des G 10 besteht mit diesem Gesetz bereits ein harmonisierter Rechtsrahmen (gem. § 1 I Befugnisse auch für LfV; vom BVerfG kompetenziell nicht in Zweifel gezogen, BVerfGE 30, 1/29 [Absatz 124]), so dass zur Harmonisierung insoweit nichts veranlasst ist. • Die AG kann gleichwohl in zwei Richtungen prüfen: o Ist sachgerecht, die Erhebung von Verkehrsdaten (§ 8a II 1 Nr. 4, 5 BVerfSchG) und Auskünfte zu dynamischer IP (§ 8d II BVerfSchG) als gegenständliche spezielle Maßnahmen abweichend zu behandeln, oder sollte der Bundesgesetzgeber dem Konzept des § 1 I G 10 folgend, auch insoweit einen einheitlichen Rechtsrahmen (auch für die LfV) schaffen, einschließlich der Erhebung sogenannter Vorratsdaten? Wären darin auch die Bestandsdatenauskünfte (ohne Eingriff in Art. 10 GG) einzubeziehen? o Ist der bundesrechtliche Befugnisrahmen wirksam oder sollten - nicht zur Harmonisierung, aber zur besseren Wirksamkeit - Änderungen erfolgen?

[1] Komplementär zu „Straftaten von erheblicher Bedeutung“ bei Strafverfolgung (§ 100g StPO)

Regelungsbeispiel:

§ X+3 Eingriff in Brief-, Post- und Fernmeldegeheimnis

(1) Die Verfassungsschutzbehörden des Bundes und der Länder dürfen dem Fernmeldegeheimnis sowie dem Brief- oder Postgeheimnis unterliegende Daten erheben, wenn tatsächliche Anhaltspunkte bestehen, dass jemand

1. *Straftaten*
   a) *… [weiter wie § 3 I S. 1 G 10; Satz 2 wird in Nummer 6 Buchstabe b) durch Aufnahme des § 129 StGB integriert]…*

   plant, begeht oder begangen hat oder
2. *in sonstiger Weise durch Bestrebungen oder Tätigkeiten nach § 3 Absatz 1 eine konkretisierte Gefahr für*
   a) *die dort genannten Schutzgüter oder*
   b) *Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse liegt,*

   verursacht.

[Tatsächliche Anhaltspunkte für eine Planung kann auch das Verhalten des Betroffenen bieten, wenn es die Annahme rechtfertigt, er werde solche Taten begehen.][2] Bei begangenen Taten gilt dies für Aufgaben nach § 3 Absatz 1 und 4 [BVerfSchG] nur, wenn, insbesondere nach den Methoden der Bestrebungen, hinreichende Anhaltspunkte dafür bestehen, dass [innerhalb eines übersehbaren Zeitraums][3] weitere Straftaten nach Absatz 1 zur Verfolgung ihrer Ziele geplant sind oder begangen werden[4].

(2) Inhalte und Umstände von Fernmeldeverkehren, die nach der Anordnung[5] nach § X+6 übertragen worden ist oder wird, dürfen auch aus einem von dem Betroffenen genutzten informationstechnischen System erhoben werden[6], wenn der Eingriff notwendig ist, um die Informationen insbesondere auch in unverschlüsselter Form zu gewinnen. An dem informationstechnischen System dürfen nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind. Sie sind bei Been-

---

[2] Die Tathandlung des „Planens“ in § 3 I G 10 bezieht sich auf ein Vorbereitungsstadium, das noch keine konkreten Vorstellungen über die Ausführung voraussetzt, sondern lediglich eine Handlungsausrichtung auf eine im Katalog des § 3 I G 10 abgebildete Unrechtsdimension (wozu ggf. auch eine „Wahlfeststellung“ getroffen werden kann, wenn die Planung Katalogdelikte einschließt, aber noch offen ist, welches zur Ausführung kommen soll). Damit ist auch die Fallkategorie der „konkretisierten“ Gefahr im Sinne einer konkretisierten persönlichen Handlungsdispositivität abgedeckt (BVerfGE 141, 220 / Rn. 112, 164). Eventuell bietet sich gleichwohl eine gesetzliche Klarstellung an, dass tatsächliche Anhaltspunkte für die Tatplanung auch bestehen, wenn das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie in überschaubarer Zukunft solche Straftaten begeht, etwa wenn eine Person aus einem Ausbildungslager für Terroristen im Ausland in die Bundesrepublik Deutschland einreist.

[3] Zusatz, inhaltlich bedeutungslos, vor dem Hintergrund der Rspr. des BVerfG aber eventuell opportun.

[4] Klarstellung der präventiven Ausrichtung der TKÜ

[5] Dies schließt insoweit Kommunikation ein, die im Zeitpunkt des Maßnahmebeginns bereits abgeschlossen ist, und geht insoweit über die bloße technische Gestaltung einer Maßnahme (als Quellen-TKÜ) hinaus.

[6] Die gegenständliche Beschränkung einer Überwachung nach dieser Befugnis ist bei der Durchführung gemäß § 9 BDSG technisch zu gewährleisten.

digung der Maßnahme, soweit technisch möglich, automatisiert rückgängig zu machen. Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. Bei jedem Einsatz sind zu protokollieren

1. *die Bezeichnung des technischen Mittels und der Zeitpunkt seines Einsatzes,*
2. *die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,*
3. *die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und*
4. *die Organisationseinheit, die die Maßnahme durchführt.*

(3) Umstände der Verkehre dürfen über Absatz 1 hinaus erhoben werden, wenn dies für die Aufgaben nach § 3 Absatz 1 Nummer 2 oder 3 oder zur Aufklärung sonstiger Bestrebungen von erheblicher Bedeutung[7] erforderlich ist. Die auf Grund des § 113b TKG gespeicherten Daten dürfen nur nach Maßgabe des Absatzes 1 erhoben werden[8].

(4) Maßnahmen nach Absatz 1 und 2 sind in der Regel nur zulässig, wenn die Erforschung des Sachverhalts mit anderen Mitteln, mit Ausnahme der Mittel nach § X+4 oder X+5, aussichtslos oder wesentlich erschwert wäre.[9]

(5) Maßnahmen dürfen sich nur

1. *in den Fällen der Absätze 1 und 2 gegen den Verdächtigen,*
2. *in den Fällen des Absatzes 3 gegen einen Beteiligten[10] oder*
3. *gegen Personen richten, zu denen hinreichende Anhaltspunkte bestehen, dass sie für den Verdächtigen oder Beteiligten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Verdächtige oder Beteiligte ihren Anschluss benutzt.[11]*

Maßnahmen, die sich auf Brief- oder Postsendungen beziehen, sind nur hinsichtlich solcher Sendungen zulässig, zu denen hinreichende Anhaltspunkte bestehen, dass sie vom Verdächtigen oder Beteiligten, herrühren oder für ihn bestimmt sind. Abgeordnetenpost von Mitgliedern des Deutschen Bundestages und der Parlamente der Länder darf nicht in eine Maßnahme einbezogen werden, die sich gegen einen Dritten richtet[12].

(6) In Antrag und Anordnung (§ X+6 Absätze 2 und 3) sind auch

---

[7] vgl. Anm. zu § X Abs. 3 S. 3

[8] Das BVerfG sieht die Erhebung der vorsorglich gespeicherten Daten nach neuerer Rsp. gleichwertig zur Inhaltsüberwachung (BVerfGE 141, 220 / Rn. 107), die es nach § 3 G 10 nicht beanstandet hat. Inhaltlich bezeichnen die Tatbestände des § 3 I G10 spezielle Sachverhalte einer konkretisierten Gefahr für die Sicherheit des Bundes. Im Interesse der Rechtsklarheit sollte begleitend auch § 113c TKG durch spezielle Aufnahme der Verfassungsschutzbehörden ergänzt werden.

[9] Konkretisierung der allgemeinen Verhältnismäßigkeitsregelung in X+1 Abs. 1 Satz 3. Eingriffe in Art., 10 GG sollen danach nur zulässig sein, wenn das Erkenntnisziel nicht oder nur wesentlich erschwert ohne solchen Eingriff erreichbar wäre. Die Mittel nach X + 4 und X + 5 (WRÜ und ODS) sind allerdings typischerweise schwerer eingreifend.

[10] vgl. § X Abs. 4 S. 1 Nr. 1

[11] Eine ausdrückliche Klarstellung, dass eine TKÜ auch durchgeführt werden darf, wenn andere Personen unvermeidbar betroffen werden, erscheint verzichtbar, da in der Maßnahme angelegt, also selbstverständlich.

[12] Geltendes Recht in § 3 II 4 G10 trotz allgemeiner Regelung in § 3b I G10. Zwar redundant/überflüssig, wegen besonderer Sensibilität der Materie gleichwohl erhalten.

1. *im Falle der Überwachung von Fernmeldeverkehren die Rufnummer oder eine andere Kennung eines zu überwachenden Anschlusses oder des Endgeräts, sofern diese nicht zugleich einem anderen Endgerät zugeordnet ist,*
2. *im Falle des Absatzes 2 auch eine möglichst genaue Bezeichnung des informationstechnischen Systems, in das zur Datenerhebung eingegriffen werden soll,*
3. *im Falle einer Überwachung des Brief- oder Postverkehrs, eine Bezeichnung der Sendungen, die der Anordnung unterliegen sollen,*

anzugeben. Abweichend von Nummer 1 genügt für die Erhebung von Umständen von Fernmeldeverkehren deren räumlich und zeitlich hinreichende Bezeichnung, sofern anderenfalls die Erreichung des Zwecks der Maßnahme aussichtslos oder wesentlich erschwert wäre[13]. Die Anordnung ist[14] auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei weitere Monate ist zulässig, soweit die Voraussetzungen der Anordnung fortbestehen. Ist die Erhebung auf Umstände der Verkehre beschränkt beträgt die Höchstdauerdauer abweichend von Satz 3 und 4 sechs[15] Monate.

(7) Die auf Grund der Anordnung erhobenen Daten dürfen durch Verfassungsschutzbehörden des Bundes und der Länder, den Militärischen Abschirmdienst und den Bundesnachrichtendienst für die in Absatz 3 Satz 1 bezeichneten Aufgaben [zur Abwehr drohender Gefahren][16] verarbeitet werden. An andere Stellen[17] dürfen sie übermittelt werden, wenn dies auf Grund hinreichender Anhaltspunkte erforderlich ist zur[18]

1. *Verfolgung von Straftaten*
   a) *in den Fällen des Absatzes 1, auch in Verbindung mit Absatz 2, und Absatz 3 Satz 2: Straftaten nach § 100a Absatz 2 StPO,*
   b) *im Falle des Absatzes 3 Satz 1: Straftaten von erheblicher Bedeutung,*
2. *Abwehr von Gefahren bei drohenden [alt.: zur Verhinderung und Verhütung von] Straftaten entsprechend Nummer 1 oder*

---

[13] Geregelt ist eine Funkzellenauskunft für gespeicherte *Verkehrsdaten* (orientiert an § 20m III 2 BKAG). Die Erhebung der nicht an eine Telekommunikation gebundenen *Standortmeldung* eines aktiv geschalteten Mobiltelefons, das sich automatisch - kommunikationsunabhängig - in einer Funkzelle einbucht, ist nicht mit einem Eingriff in das Fernmeldegeheimnis verbunden, erfolgt mithin aufgrund allgemeiner Erhebungsbefugnisse, nicht nach § X+5.

[14] in § 8b I 3 BVerfSchG ist eine klarstellende Einschränkung „für künftig anfallende Daten“ aufgenommen, die allerdings verzichtbar erscheint. Geregelt wird die Gültigkeitsdauer der Anordnung. Hieraus folgt zugleich eine zeitliche Beschränkung für künftig anfallende Daten. Umgekehrt betrifft die Befristung dem Regelungsgegenstand nach (Anordnungsgültigkeit) nicht den Erhebungsgegenstand, also auch nicht dem Zeitraum bereits in der Vergangenheit anfallender, im Anordnungszeitraum vorliegender Informationen. Hierzu erscheint eine spezielle Klarstellung verzichtbar (vgl. in jüngerer Gesetzgebung § 53 III BKAG).

[15] Die Regelung folgt dem neuen Modell des § 53 III BKAG.

[16] Der Zusatz berücksichtigt die Verweisung des § 4 II 3 G10 auf § 1 I G10 mit dem dort aufgenommenen Bezug auf drohende Gefahren. Da die in § 3 I BVerfSchG aufgeführten Bestrebungen/Tätigkeiten jeweils bereits drohende Gefahren für die dort aufgeführten Schutzgüter bezeichnen, erscheint der Zusatz allerdings redundant und somit verzichtbar.

[17] wie § 4 IV G10-G: andere Verfassungsschutzbehörden sind keine anderen Stellen in diesem Sinne.

[18] Trias orientiert sich an § 4 IV G 10.

3. *Vorbereitung und Durchführung eines Verfahrens nach Artikel 21 Abs. 2 Satz 2 des Grundgesetzes oder einer Maßnahme nach § 3 Abs. 1 Satz 1 des Vereinsgesetzes.*

In den Fällen des Absatzes 1, auch in Verbindung mit Absatz 2, und Absatz 3 Satz 2 kann zur Gefahrenabwehr und Strafverfolgung bei dringendem Verdacht[19] auch wegen sonstiger drohender oder begangener Staatsschutzdelikte (§ 20 Absatz 1 Satz 2 [BVerfSchG]) von erheblicher Bedeutung übermittelt werden.

(8) Das Grundrecht des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10 des Grundgesetzes) wird durch diesen Paragraphen sowie § X+11 Absatz 1 Satz 2 eingeschränkt[20].

(9) Gegen Anordnung und Vollzug der Maßnahmen ist der Rechtsweg vor der Mitteilung an den Betroffenen (§ X+10) ausgeschlossen.

[19] Die Gesamtwürdigung der Verhältnismäßigkeit muss sowohl Schutzgut wie auch Erkenntnisdichte einbeziehen. Bei hoher Erkenntnisdichte wäre zumindest im Bereich der spezifischen Schutzaufgabe des Verfassungsschutzes rechtsstaatlich unerträglich, wenn der Staat sehenden Auges den Störungsverlauf geschehen lassen muss. Ebenso kann bei der Strafverfolgung das rechtsstaatliche Verfolgungsinteresse höher gewichtet werden, wenn keine Anschlussermittlungen mit Streubreite initiiert werden, sondern der Verdacht bereits sehr verdichtet ist. In der Rsp. des BVerfG ist dies noch nicht judiziert, aber angelegt. Die Rechtsgüterbetrachtung im BKAG-Urteil ist auf bloße Spurenansätze bezogen. Die Beschränkung auf Staatsschutzdelikte trägt der dies betreffenden Fachkunde der Verfassungsschutzbehörden Rechnung, die nicht in gleicher Weise bei sonstigen Delikten der Allgemeinkriminalität gegeben ist.
Allerdings ist der Begriff des „dringenden" Verdachts, der § 112 I 1 StPO entlehnt ist, möglicherweise missverständlich im Hinblick auf die terminologisch ähnliche „dringende" Gefahr iSd Art. 13 IV GG / § X+4 Abs. 1 Nr. 2. Auch dort bezeichnet der Begriff „dringend" u.a. eine erhöhte Erkenntnisdichte, die allerdings unterhalb der Schwelle eines dringenden Verdachts iSd § 112 StPO bleibt. Eventuell sollte hier somit doch ein anderer Begriff gewählt werden (da er in § X+4 Abs. 1 Nr. 2 zum Andocken an Art. 13 IV GG „gesetzt" ist).

[20] Zitate ggf. vorzugswürdig (auch zu § X+5) in gesondertem Paragraphen.

5 Eingriff in informationstechnische Systeme

Version 29.08.2017

Voraussetzungen	Sachverhalt	• Besonders schwere Gefahr (§ X+4 Abs. 1), angeglichen an WRÜ[1]
	Erkenntnisse	• verdichteter Verdacht (hinreichende Anhaltspunkte)
	Verfahren	• Wie G 10 (zusammengefasst in §§ X+6 ff geregelt)
Richtung		• Handlungs- oder Zustandsverantwortlicher (§ X+4 Abs. 2)
Folgen	Zweckbind.	• Besonders schwere Gefahren/Straftaten drohen konkretisiert
	Mitteilungen	• Ähnlich G 10 (§ X+10)

Erläuterung	• Klärungsbedürftig, ob praktischer Bedarf für spezielle Regelung zu begrenzten Eingriffen besteht und - bei Bedarf - dafür mindere Anforderungen gestellt werden könnten[2]. • Schutzbereich und Eingriffsqualifikation sind im Näheren zu klären/präzisieren, z.B.: o Schutz der Inhalte von Speichermedien abhängig von Einbindung in IT-System? o Auslesen beschlagnahmter IT-Systeme grundlegend anders zu würdigen, allein weil offene Maßnahme? o Zugang auf regulärem Weg (Passwortanmeldung) Eingriff, wenn unbefugt (Passwort über Quelle beschafft)? o Überwachung von Maschinenkommunikation zur Aufklärung elektronischer Angriffe (vgl. auch X+4 Abs. 5).

[1] Die Regelung berücksichtigt die neuere Rechtsprechung des BVerfG, speziell auch mit dem im künftigen § 100b StPO aufgegriffenen Ansatz, den Eingriff in das informationstechnische System dem Eingriff in die Unverletzlichkeit der Wohnung vergleichbar bzw. entsprechend zu gewichten (BVerfGE 141, 220 / Rn. 192, 210 a.E.; ferner 105, 115, 238; das Gericht sieht in seinem Urteil ausdrücklich eine Fortentwicklung seiner vorangegangenen Rechtsprechung, Rn. 292).

[2] Begrenzte Eingriffen sind nicht geprägt von dem Gefährdungspotenzial, das das BVerfG bei der Konstruktion des besonderen Schutzes informationstechnischer Systeme als die Verhältnismäßigkeitsrelation typisierend zu Grunde gelegt hat: „Ein staatlicher Zugriff auf einen derart umfassenden Datenbestand ist mit dem naheliegenden Risiko verbunden, dass die erhobenen Daten in einer Gesamtschau weitreichende Rückschlüsse auf die Persönlichkeit des Betroffenen bis hin zu einer Bildung von Verhaltens- und Kommunikationsprofilen ermöglichen“ (BVerfGE 120, 274 / Rn. 232). Bei der technischen Auswertung elektronischer Speicherung ist die Datenerhebung bereits mit dem technischen Suchprofil zu begrenzen, was zugleich den Eingriffsgehalt begrenzt (vgl. BVerfGE 120, 378 und BVerwG 6 C 7.13 vom 22.10.2014). Aus der Schutzzweckperspektive ist nicht ohne weiteres schlüssig, isoliert dem Umfang der Speicherung Relevanz zur Qualifikation des Eingriffsgehalts zuzumessen, vielmehr erscheint erst der Umfang der Datenerhebung konstitutiv für die besondere Eingriffsdimension. Es erschließt sich nicht, weshalb das Speichermedium oder ein - nicht zur Kenntnis genommener, nur technisch abgeglichener - Speicherzusammenhang schutzwürdigkeitsrelevant sein sollte. Eine andere Sicht würde auch grundlegende Fragen zum Grundrechtsträger, etwa bei Eingriffen in eine Cloud stellen.

Regelungsbeispiel:

§ X+4 Eingriff in informationstechnische Systeme

(1) Die Verfassungsschutzbehörde darf heimlich personenbezogene Daten aus einem informationstechnischen System erheben, wenn hinreichende Anhaltspunkte vorliegen für eine konkretisierte[3] dringende[4] Gefahr für

1. *die in § 3 Absatz 1 [BVerfSchG][5] genannten Schutzgüter,*
2. *die Funktionsfähigkeit kritischer Infrastrukturen[6] oder*
3. *Leib, Leben oder Freiheit einer Person[7].*

Satz 1 Nummer 1 liegt insbesondere vor, wenn hinreichende Anhaltspunkte bestehen, dass jemand eine Straftat nach[8]

1. *§§ 81, 82, 94, 95 Absatz 3, § 96 Absatz 1, § 98 Absatz 1 Satz 2, § 99 Absatz 2 und §§ 100, 100a Absatz 4 des Strafgesetzbuches plant,*
2. *§§ 89a, 89c Absatz 1 bis 4, § 129 Absatz 4, wenn der Zweck oder die Tätigkeit der kriminellen Vereinigung auf politisch motivierte Gewalttaten gerichtet ist[9], § 129a Abs. 1, 2, 4, 5 Satz 1 Alternative 1, jeweils auch in Verbindung mit § 129b Abs. 1 des Strafgesetzbuches begangen hat und seine auf Gewaltanwendung gerichteten Bestrebungen fortsetzt.*

(2) Die Maßnahme darf sich nur gegen Personen richten, zu denen hinreichende Anhaltspunkte bestehen, dass

---

[3] BVerfGE 141, 220, Rn. 213

[4] Zur wertenden Ausfüllung der Anforderung einer „dringenden" Gefahr (Art. 13 Abs. 4 GG) bieten die Konkretisierungen in Nummer 1 auch bei der Anwendung der Nummer 2 einen leitbildhaften Anhalt. Unter Berücksichtigung von Nummer 1 Buchstabe a) ist beispielsweise auch bei Proliferationsaktivitäten oder elektronischen Sabotageangriffen fremder Mächte von einer „dringenden Gefahr" nach Nummer 2 Buchstabe a) auszugehen. Gleiches gilt unter Berücksichtigung von Nummer 1 Buchstabe b) bei besonders schweren Fällen politisch motivierter Kriminalität unabhängig davon, ob hinreichende Anhaltspunkte für ein Vorgehen einer Vereinigung bestehen. Solche besonders schweren Fälle können beispielsweise vorliegen, wenn die Taten im besonderen als Angriff auf die grundgesetzliche Werteordnung typisiert sind, so etwa, wenn sie mit rassistischem Ansatz das friedliche Zusammenleben der unterschiedlichen Bevölkerungsgruppen in Frage stellen, weil sie einem Teil der Bevölkerung das Recht abspricht, gleichberechtigt am gesellschaftlichen Leben teilzunehmen, und damit geeignet sind, den öffentlichen Frieden qualifiziert zu stören.In diesem Fall liegt eine konkrete Gefahr für die Sicherheit des Staates unabhängig davon vor, dass auch bereits eine konkrete Gefahr für eine Folgetat gegen Individualrechtsgüter vorliegt.

[5] Einbezogen in der Verweisung auf § 3 I BVerfSchG sind neben den Schutzgütern des Bestandes und der Sicherheit des Staates auch deren spezielle Ausformungen mit der freiheitlich demokratischen Grundordnung (als Grundlage der staatlichen Ordnung) sowie der Völkerverständigung (als Grundlage der wertegebundenen Einordnung Deutschlands in die Staatengemeinschaft)

[6] Der Begriff ist mit § 2 X BSIG in die Rechtsordnung eingeführt und mit der BSI-KritisV näher definiert. Diese Legaldefinition gilt unmittelbar nur für den Vollzug des BSIG, gibt darüber hinaus aber ein auch für die vorliegende Regelung heranzuziehendes Leitbild, da die Rechtsbegriffe funktional entsprechend verwendet werden.

[7] Da die Aufklärung generell voraussetzt, dass die Verfassungsschutzaufgabe nach § 3 I BVerfSchG eröffnet ist, ist vorliegend keine ergänzende Regelung zur verfassungsschutzrelevanten Qualifikation der Gefahr erforderlich.

[8] Nummer 1 bezeichnet spezielle Sachverhalte konkretisierter Gefahren für die Sicherheit des Bundes. Hätte der Staat nicht die Mittel, solche Sachverhalte aufzuklären, um schwere Staatsschutzdelikte zu verhindern, wären die Grundlagen staatlicher Funktionsfähigkeit gefährdet und insbesondere das Vertrauen der Bürger erschüttert, dass sie in Deutschland individuell vor Terrorakten und ihr Staat - als demokratische Organisation grundlegender Kollektivanliegen - vor Ausforschung und Angriffen fremder Mächte geschützt sind. Die Befugnis gewinnt mit der Anknüpfung an Störungssachverhalte, die den besonderen Bestimmtheitsanforderungen von Strafnormen unterliegen, wesentlich an Rechtsklarheit und Praxistauglichkeit. Die Auswahl der speziell benannten Tatbestände berücksichtigt deren besondere Praxisbedeutung.

[9] Die Aufnahme des § 129 Absatz 4 StGB ohne Beschränkung auf dessen 2. Halbsatz weicht bewusst davon ab, lediglich Katalogtaten nach § 100c Absatz 2 StPO aufzunehmen. Anders als im Bereich der Strafverfolgung können hier für Zwecke der Gefahrenabwehr über den Strafrahmen hinaus weitere Gesichtspunkte zur Qualifikation eines besonderen Gewichts der Gefahr herangezogen werden. Vorliegend ist maßgeblich, dass bei besonders schweren Fällen organisiert betriebener politisch motivierter Kriminalität ebenfalls eine dringende Gefahr für die Sicherheit des Staates besteht. Dies ist generell bei organisiert betriebenen, politisch motivierten Gewalttaten anzunehmen, weil hierin zugleich ein massiver Angriff auf Grundlagen der Demokratie liegt, die auf friedlicher Teilhabe beruht und nur in diesem Friedensrahmen auch funktionsfähig ist.

1. *sie die Straftat planen oder begangen haben oder an den bezeichneten Bestrebungen oder Tätigkeiten beteiligt sind,*
2. *in ihrem informationstechnischen System Personen nach Nummer 1 Informationen verarbeiten und die Erforschung des Sachverhalts nicht ebenso durch eine Maßnahme nach Nummer 1 möglich ist.*

Die Maßnahme darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden. [Soweit möglich, ist technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden.][10]

(3) In Antrag und Anordnung (§ X+6 Absätze 2 und 3) ist auch eine möglichst[11] genaue Bezeichnung des informationstechnischen Systems, in das zur Datenerhebung eingegriffen werden soll, anzugeben. Die Anordnung ist auf höchstens einen Monat zu befristen. Eine Verlängerung um jeweils nicht mehr als einen weiteren Monat ist zulässig, soweit die Voraussetzungen der Anordnung fortbestehen.

(4) Die Verfassungsschutzbehörde darf

1. *die nach Absatz 1 erhobenen personenbezogenen Daten zur Aufklärung eines dort bezeichneten Verdachts verarbeiten[12] und*
2. *[13]Erkenntnisse aus der Verarbeitung nach Nummer 1 übermitteln, wenn hinreichende Anhaltspunkte bestehen, dass dies*
   a) *zur Abwehr einer in Absatz 1 bezeichneten drohenden[14] Gefahr oder*
   b) *zur Verfolgung einer in § 100b Abs. 1 der Strafprozessordnung[15] genannten Straftat*

erforderlich ist.

---

[10] Folgt bereits aus der Erforderlichkeit bzw. sparsamer Datenverarbeitung. Wird hier im Zusammenhang geregelt und nicht vor die Klammer gezogen, da sie sich auf eine Maßnahme der technischen Überwachung bezieht, bei der das BVerfG besonders die Gefahr einer umfassenden Ausleuchtung der Persönlichkeit des Betroffenen betont hat. Der Gesetzesanwender wird durch die klarstellende Regelung zu einer grundrechtsschonenden Durchführung der Maßnahme angehalten. Der allgemeine Grundsatz beansprucht ohnehin unmittelbare Geltung für die Ausübung aller Befugnisse.

[11] In der AG wurde überlegt, stattdessen zu formulieren: „soweit möglich zu bezeichnen“. Nach nochmaliger Prüfung wird vorgeschlagen, am ursprünlichen wording, das den bestehenden Regelungen in § 20k BKAG a.F. bzw. § 49 BKAG n.F. entspricht festzuhalten, um Angriffsflächen oder Diskussionen, ob etwas anderes gemeint ist, zu vermeiden.

[12] Der Begriff „verarbeiten“ greift bereits die neuen Datenschutzbegriffe der Datenschutz-Grund-VO (EU) 2016/679 auf, die mit dem Datenschutz-Anpassungs- und -Umsetzungsgesetz EU auch im Bundesverfassungsschutzgesetz übernommen werden. Der Begriff schließt also in bisheriger Terminologie auch die Nutzung der Daten ein. Der Bezug auf einen in Absatz 1 bezeichneten Verdacht beschränkt die Verwendung nicht auf die Aufklärung des Anlassverdachts setzt bei Zweckänderung aber ebenfalls einen entsprechenden Katalogtatenverdacht voraus und ebenso die Erkenntnisanforderung der „hinreichenden Anhaltspunkte“.

[13] Ebenso bezieht der Verweis in Nummer 2 Buchstabe a) auf eine in Absatz 1 bezeichnete Gefahr im Falle des Absatzes 1 Nummer 2 die Qualifikation als dringende Gefahr ein. Im Übrigen ermöglicht Nummer 2 lediglich die Übermittlung von Erkenntnissen, also nicht eine Übermittlung von noch nicht ausgewerteten Rohdaten. Demgemäß muss der Übermittlung eine konkrete Erforderlichkeitsprüfung vorausgehen, die Erforderlichkeit kann nicht bereits dem Erhebungsgegenstand entnommen werden. Geregelt werden lediglich Erkenntnisse aus der Verarbeitung der aus der Maßnahme gewonnenen Informationen. Neue Erkenntnisse, die sich im Weiteren als Schlussfolgerung aus der Zusammenführung mit sonstigen Informationen ergeben, sind bereits nicht von der besonderen Zweckbindung der mit der Maßnahme erhobenen Informationen umfasst.

[14] Mit dem Begriff der „drohenden“ Gefahr wird verdeutlicht, dass die Nutzung als Spurenansatz zur allgemeinen Lageerforschung nicht genügt, sondern nach Erkenntnislage eine Gefahr bereits im Einzelfall besteht oder immerhin konkretisiert zu entstehen droht (vgl. BVerfGE 141, 220 / Rn. 283), also die konkreten situativen oder individuellen Umstände solche Gefahren absehbar machen (vgl. BVerfG a.a.O. / Rn. 112).

[15] Künftige StPO-Regelung der ODS

(5) § X+3 Absatz 2 Sätze 2 bis 5 gelten entsprechend und auch dann[16], wenn der Eingriff in ein informationstechnisches System ausschließlich erfolgt, um andere Informationen als personenbezogene Daten zu erheben.

[16] Der Regelung geht davon aus, dass solcher Eingriff im Übrigen nicht an § X+4 zu messen ist und bedarf insoweit noch gründlicher verfassungsrechtlicher Prüfung, vgl. Fn. 2. Sie dient u.a. der Detektion von Maschinenkommunikation, also dem Aufspüren von Schadsoftware.

6 Eingriffe in Art. 13 GG

Version 29.08.2017

Erläuterung	• Parallelisiert mit Eingriffen in informationstechnische Systeme, Näheres daher dort. • Im Interesse einheitlicher Verfahren ist auch vorliegend die Entscheidung der Kommission vorgesehen, nicht eines Gerichts der ordentlichen Gerichtsbarkeit. Der durch die Kommission gebotene Rechtsschutz ist materiell und verfahrensmäßig der gerichtlichen Kontrolle gleichwertig[1]. Gleichwohl bedarf diese Gestaltung im Hinblick auf Art. 13 Abs. 4 und Abs. 5 Satz 2 GG noch näherer Prüfung.

Regelungsbeispiel:

§ X+5 Heimliche Datenerhebung aus Wohnungen

(1) Die Verfassungsschutzbehörde darf heimlich[2], auch unter Einsatz technischer Mittel, personenbezogene Daten aus einer Wohnung entsprechend § X+4 Absatz 1 erheben, soweit aufgrund tatsächlicher Anhaltspunkte, insbesondere zu der Art der zu überwachenden Räumlichkeiten und dem Verhältnis der zu überwachenden Personen zueinander, anzunehmen ist, dass durch die Überwachung Äußerungen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, nicht erfasst werden. Auf die erhobenen Daten ist § X+4 Absatz 4 entsprechend anzuwenden[3]. Stimmt der

[1] BVerfG vom 20.09.2016 - 2 BvE 5/15 - (Rn. 38, 46), allerdings ein Kontrollorgan eigener Art außerhalb der rechtsprechenden Gewalt (Rn. 41). Nach dem Telos des Art. 13 IV GG dürfte funktionell richterliche Kontrolle vorausgesetzt sein, die ebenso von der Kommission gewährleistet ist. Umfassend zur judikativen Tätigkeit der Kommission: Huber, in Schenke/Graulich/Ruthig, SiR, § 15 G 10 Rn. 5 ff. Auch im BKAG-Urteil stellt das BVerfG(E 141, 220 / Rn. 117, 174) - nicht speziell zur WRÜ - auf eine „unabhängige Instanz“ ab und erwähnt nur beispielhaft („etwa“) Gericht bzw. Richter. Aus grundrechtlicher Schutzperspektive ist unter der vom BVerfG gesehenen Problematik „additiver“ Eingriffe vorzugswürdig, wenn die unabhängige Kontrolle fallbezogen über sämtliche Intensiveingriffe bei einer Instanz liegt und nicht maßnahmebezogen auf verschiedene Instanzen (Kommission/Gericht) verteilt ausgeübt wird. Der umfassende, über gerichtliche Anordnungskontrolle hinaus gehende Schutzansatz der Kommission (§ 15 Abs. 5 Satz 2 G 10) prädestiniert sie zu einer solchen fallbezogenen Kontrolle. Beim physischen Zugriff auf den Rechner wäre andernfalls die Befugnis für die Infiltration des IT Systems bei der Kommission, für das Betreten der Räumlichkeit dagegen müsste ein Antrag bei Gericht eingereicht werden. Eine einheitliche Maßnahme würde dadurch gerade sinnwidrig aufgespaltet. Zudem besitzt die Kommission aufgrund laufender Befassung spezifische Fachkunde in nachrichtendienstlichen Angelegenheiten, die gleichwertig bei den Gerichten nicht vorhanden ist.

[2] Dies schließt den Zutritt zur Wohnung ohne Kenntnis des Wohnungsinhabers ein (nicht nur technische Überwachung). Hat der Wohnungsinhaber hingegen eingewilligt, liegt kein Eingriff in Art. 13 GG vor (auch wenn er über den Zweck des Aufenthalts irrt - der spezifische Schutzbereich des Rechts auf Wohnung erfasst nicht das Vertrauen in die Redlichkeit der Personen, die in die eigene Wohnung eingeladen werden), so dass dazu keine spezielle Regelung erforderlich ist. Im Interesse der Rechtsklarheit erfolgt gleichwohl eine Klarstellung in den Sätzen 3 und 4.

[3] Klärungsbedürftig ist, ob zum Kernbereichsschutz auf der Verwertungsebene die allgemeine Regelung in § X+1 Abs. 3 reicht oder speziell zur WRÜ eine umfassende - nicht auf Zweifelsfälle beschränkte - Vorabprüfung durch eine unabhängige Kontrollinstanz erforderlich ist (vgl. BVerfGE 141, 220 / Rn. 200, 204). Bei der Anpassung der StPO ist der Gesetzgeber zuletzt nicht davon ausgegangen, vielmehr hat er die bisherige Regelung in § 100c Abs. 5 Satz 6 StPO a.F. inhaltlich im neuen § 100d Abs. 4 Satz 5 StPO n.F. insoweit übernommen, als lediglich einzelfallbezogen („soweit für bereits erlangte Erkenntnisse ein Verwertungsverbot nach Absatz 2 in Betracht kommt“) eine Entscheidung des Gerichts herbeizuführen ist.
Sollte eine spezielle Regelung erforderlich sein, wäre zu erwägen, sie auf „Privatwohnungen“ zu beschränken, also Wohnungen im engeren Sinne. Nicht eingeschlossen wären Betriebs- oder Geschäftsräume, die nach der Rspr. des BVerfG typischerweise nicht privater Rückzugsort des Einzelnen sind (BVerfGE 141, 220, Rn. 180), ebenso gesonderte Funktionsräume wie Garagen und Kellerräume usw.

Betroffene dem Zutritt zur Wohnung zu, findet Absatz 4 Anwendung. Die Vorschriften über verdeckte Ermittlungen bleiben in diesem Fall unberührt.

(2) Die Maßnahme darf sich nur gegen Personen richten, zu denen hinreichende Anhaltspunkte bestehen, dass sie die Straftat planen oder begangen haben oder an den bezeichneten Bestrebungen oder Tätigkeiten beteiligt sind. In Wohnungen anderer Personen ist die Maßnahme nur zulässig, wenn hinreichende Anhaltspunkte bestehen, dass sich eine in Satz 1 genannte Person in ihr aufhält und der Zweck der Maßnahme nicht unter Beschränkung auf deren Wohnung zu erreichen ist.

(3) In Antrag und Anordnung (§ X+6 Absätze 2 und 3) sind auch die zu überwachende Wohnung oder die zu überwachenden Wohnräume anzugeben. Die Anordnung ist auf höchstens einen Monat zu befristen. Eine Verlängerung um jeweils nicht mehr als einen weiteren Monat ist zulässig, soweit die Voraussetzungen der Anordnung fortbestehen.

(4) Im unmittelbaren zeitlichen Zusammenhang mit dem Einsatz von Personen in einer Wohnung für die Verfassungsschutzbehörde darf sie in oder aus der Wohnung Daten mit technischen Mitteln erheben, wenn dies zur Abwehr von Gefahren für deren Leib, Leben oder Freiheit unerlässlich ist[4]. Die erhobenen personenbezogene Daten dürfen nur zum Zweck der Eigensicherung nach Satz 1, sonstiger Gefahrenabwehr, einschließlich der Aufgaben nach § 3 Absatz 1 [BVerfSchG], oder der Strafverfolgung verarbeitet werden. Die Verarbeitung zur sonstigen Gefahrenabwehr oder der Strafverfolgung setzt die Feststellung der Rechtmäßigkeit der Maßnahme durch die Kommission [nach § 15 des Artikel 10-Gesetzes] voraus; § 15 Absatz 6 Satz 2 G 10[5] gilt entsprechend. Auf die Feststellung sind §§ X+7 und 8 anzuwenden.

(5) Die Verfassungsschutzbehörde darf heimlich Wohnungen auch betreten, um Maßnahmen nach den Absätzen 1 und 4 oder Maßnahmen nach § X+3 Absatz 2 oder § X+4 vorzubereiten. Im Fall des Absatzes 4 ist dazu eine Anordnung entsprechend Absatz 3 erforderlich. In den Fällen der § X+3 Absatz 2 oder § X+4 muss dies in der Anordnung oder durch Ergänzungsanordnung erlaubt sein. Heimlich betreten werden darf nur die Wohnung dessen, gegen den sich die Überwachungsanordnung richtet.

(6) Das Grundrecht der Unverletzlichkeit der Wohnung (Artikel 13 des Grundgesetzes) wird durch diesen Paragraphen eingeschränkt.

---

[4] Die innerbehördliche Zuständigkeit für die Entscheidung zum Einsatz technischer Eigensicherung ist gem. § X+6 Abs. 1 Satz 1 in der DV nd-Mittel zu regeln. Alternativ (modularer Ansatz) kommt auch gesetzliche Regelung in Betracht. Entsprechende Regelungen - z.B. § 28a Abs. 3 BPolG oder Art. 11 Abs. 4 Satz 1 BY VSG - sehen eine Zuständigkeit der Behördenleitung, teils mit Eilfallzuständigkeit der Abteilungsleitung vor.

[5] Verweisung ist anzupassen, wenn Regelung in das Verfassungsschutzgesetz übernommen wird.

7 Mitwirkungspflichten

Version 29.08.2017

Voraussetzungen	Sachverhalt	• Soweit die Verfassungsschutzbehörde befugt ist, Daten, die Gegenstand eines Vertragsverhältnisses von Luftverkehrsunternehmen, Kreditinstituten oder Post-/TK-/Telemedienunternehmen sind, zu erheben, sind die Unternehmen bei der Erhebung mitwirkungspflichtig. • Unter den Voraussetzungen einer Quellen-TKÜ oder Onlinedurchsuchung sind TK-Unternehmen mitwirkungspflichtig, die dazu nötige Software im informationstechnischen System der Zielperson aufzubringen. • Die Mitnutzung von Videoüberwachungseinrichtungen, die im besonderen öffentlichen Sicherheitsinteresse betrieben werden (§ 6b I 2 BDSG), ist in qualifizierten Fällen (BO von erheblicher Bedeutung) zu ermöglichen, darf zur gezielten Überwachung bestimmter Personen aber nur entsprechend den Regelungen zur technischen Observation eingesetzt werden.
	Erkenntnisse	• Gemäß den Erhebungsbefugnissen, zu denen die Mitwirkung Annex ist
	Verfahren	• Gemäß den Erhebungsbefugnissen, zu denen die Mitwirkung Annex ist
Richtung		• Gemäß den Erhebungsbefugnissen, zu denen die Mitwirkung Annex ist, hilfsweise gem. der allgemeinen Regelung für individualisierte ND-Mittel in § X Absatz 4
Folgen	Zweckbind.	Entfällt. Geregelt wird nur die Mitwirkung. Die Datenverarbeitung folgt den einschlägigen Erhebungs- und Verwendungsnormen.
	Mitteilungen	Entfällt. Geregelt wird nur die Mitwirkung. Die Datenverarbeitung folgt den einschlägigen Erhebungs- und Verwendungsnormen.

Regelungsbeispiel:

§ X+11 Mitwirkungspflichten

(1) Die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses[1] (Bestandsdaten) gespeicherten Daten haben

1. *Luftfahrtunternehmen,*
2. *Unternehmen der Finanzbranche[2],*
3. *diejenigen, die geschäftsmäßig Post-, Telekommunikations- oder Telemedien-dienste erbringen*

der Verfassungsschutzbehörde auf Verlangen zu übermitteln, wenn die Auskunft zur Erfüllung ihrer Aufgaben erforderlich ist. Zur Auskunft nach Nummer 1 sind ebenso die Betreiber von Computerreservierungssystemen und Globalen Distributionssystemen verpflichtet[3]. Besondere Vorschriften, insbesondere über die jeweils mitzuteilenden Datenarten, bleiben unberührt[4]. Die Auskunft nach Nummer 3 darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden (§ 113 Absatz 1 Satz 3 des Telekommunikationsgesetzes). Dient eine Auskunft ausschließlich der Vorbereitung von Folgemaßnahmen, darf sie nur nach Maßgabe der dafür geltenden Regelungen verlangt werden[5]. Die Verfassungsschutzbehörde kann die zur Erfüllung ihrer Aufgaben erforderlichen Bestandsdaten auch durch Ersuchen um Abruf an das Bundeszentralamt für Steuern nach § 93b Absatz 1 der Abgabenordnung und die Bundesnetzagentur nach § 112 Absatz 2 des Telekommunikationsgesetzes erheben.

(2) Absatz 1 Satz 1, auch in Verbindung mit Satz 2, gilt für die dort Verpflichteten ebenso zu den Umständen und Inhalten der von ihnen erbrachten Leistungen[6], wenn die Auskunft zur Aufklärung von Bestrebungen von erheblicher Bedeutung erforder-

---

[1] Die Regelung gilt für den geregelten Lebenssachverhalt ohne weitere Einschränkungen im Anwendungsbereich. Allerdings muss der Sachverhalt deutscher Jurisdiktion unterliegen, was einen genuinen Bezug zum Bereich deutscher Souveränität voraussetzt. Dieser ergibt sich auch aus einer Leistungserbringung in Deutschland (Marktortprinzip). Ein inländischer Sitz des leistungserbringenden Unternehmens ist hingegen nicht notwendig, allerdings ist bei Auslandssitz die nach deutschem Recht bestehende Pflicht unter Umständen nicht effektiv durchsetzbar. Dem wäre dann durch internationale Zusammenarbeit abzuhelfen

[2] Die im bisherigen § 8a Abs. 2 Nr. 2 BVerfSchG benannten „Kreditinstitute, Finanzdienstleistungsinstitute und Finanzunternehmen“ sind nach der Legaldefinition in § 1 KWG wohl zu eng. Umfasst sein müssen alle Unternehmen der Finanzbranche, bspw. auch Kreditkartenunternehmen, Transferdienstleister, E-Geldunternehmen oder auch Dienstleister neuer Zahlungsmöglichkeiten, wie beispielsweise die Bitcoin Deutschland GmbH. Näheres - speziell zur angemessenen Begrifflichkeit - bleibt in Abstimmung mir den Finanzressorts zu klären.

[3] Abweichend vom bisherigen § 8a II 1 Nr. 1 BVerfSchG werden die Betreiber von Computerreservierungssystemen und Globalen Distributionssystemen hier getrennt geregelt, da Satz 1 die Angaben zum Vertragsverhältnis des Verpflichteten bezieht, das im Falle der Betreiber von Computerreservierungssystemen und Globalen Distributionssystemen mit den Luftffahrtunternehmen besteht. Diese Vertragsdaten sind hier nicht relevant, vielmehr geht es um die in den Reservierungssystemen gespeicherten Angaben zu den Kunden der Luftfahrtunternehmen.

[4] So regelt etwa § 113 TKG abschließend den Datenkranz, der zu beauskunften ist.

[5] Das BVerfG (E 130, 151 / Rn. 185) hat zu § 113 Absatz 1 Satz 2 TKG die Auffassung vertreten, dass die allgemeine Erhebungsvoraussetzung der Erforderlichkeit insoweit nicht zureichend klar sei. Daher wird hier vorsichtshalber eine ausdrückliche Regelung dazu aufgenommen (allgemein bereits in § A Abs. 2). Die weitere Verfahrensregelung im derzeitigen § 8d II 2 BVerfSchG erscheint dagegen überflüssig und soweit die Daten für Nutzungen benötigt werden, für die keine besonderen Verfahrensaussetzungen im Sinne der Regelung gelten, auch überschießend.

[6] In der Gesetzesbegründung kann dies mit den im bisherigen § 8a I 1 BVerfSchG aufgeführten Datenarten näher erläutert werden.

lich und das …amt für Verfassungsschutz, insbesondere nach § X+3, zur Erhebung der Daten befugt ist[7].

(3) § X Absatz 4 gilt entsprechend, soweit für die jeweilige Erhebung keine speziellen Regelungen gelten[8].

(4) Die Betreiber einer Videoüberwachung nach § 6b Absatz 1 Satz 2 des Bundesdatenschutzgesetzes sind verpflichtet, der Verfassungsschutzbehörde die Überwachung auszuleiten und Aufzeichnungen zu übermitteln, wenn dies zur Aufklärung von Bestrebungen von erheblicher Bedeutung erforderlich ist. Die Maßnahme darf nur unter den Voraussetzungen des § X Absatz 4 Satz 1 gegen eine Person gerichtet werden.

[[9](5) Das Bundesministerium des Innern wird ermächtigt, durch Rechtsverordnung im Einvernehmen mit dem Bundeskanzleramt, dem Bundesministerium für Wirtschaft und Energie, dem Bundesministerium für Verkehr und digitale Infrastruktur, dem Bundesministerium der Justiz und für Verbraucherschutz und dem Bundesministerium der Verteidigung ohne Zustimmung des Bundesrates[10] zu bestimmen, dass die Verpflichteten

1. *an angeordneten Maßnahmen nach § X+3 und § X+4 technisch mitwirken[11], insbesondere durch*
   a) *Ausleitung von Telekommunikation nach § X+3 Absatz 1,*
   b) *Zugangsgewährung zur Ausleitung nach Buchstabe a,*
   c) *Einbringen von technischen Mitteln zur Durchführung von § X+3 Absatz 2 oder § X+4,*
2. *zur Durchführung der Mitwirkung nach Nummer 1 Personen zu betrauen haben, die einer einfachen Sicherheitsüberprüfung (§ 8 des Sicherheitsüberprüfungsgesetzes) unterzogen sind,*
3. *Informationen, soweit dazu keine Regelungen auf Grund § 110 des Telekommunikationsgesetzes getroffen werden[12], ganz oder teilweise auf maschinell verwertbaren Datenträgern oder durch Datenfernübertragung übermitteln müssen. Dabei können insbesondere geregelt werden*

---

[7] Die besonderen Voraussetzungen nach § X+3 gelten nur in seinem Anwendungsbereich, also für Daten, die dem Schutz des Art. 10 GG unterliegen. Dies ist für Standortdaten, die ein TK-Unternehmen beim Mobilfunk nicht im Zusammenhang mit Kommunikationsverkehren erhebt (um die Einbuchung eines aktiv geschalteten Mobiltelefons im VLR bzw. MSC zu erfassen) nicht der Fall. Die Erhebungsbefugnis solcher Daten folgt aus § A Abs. 1, wobei die Auskunftsverpflichtung gem. § X+11 Abs. 3 auf BO von erheblicher Bedeutung beschränkt ist (im Ergebnis entsprechen die Voraussetzungen - unter Einbezug von Absatz 4 - also denen der technischen Observation nach § X, was wertungskonsistent ist). Dies könnte in einer Gesetzesbegründung klarstellend erläutert werden, bedarf aber keiner speziellen Regelung im Gesetz (da nach Wortlaut und Systematik eindeutig).

[8] Dies ermöglicht auch Gruppenauskünfte, wie Passagierlisten oder Funkzellenabfrage, wenn sich die tatsächlichen Anhaltspunkte auf den gruppenbildenden Sachverhalt beziehen, also für alle Gruppenangehörigen vorliegen (z.B. Anhaltspunkte, dass sich die Zielperson in einer Gegend aufgehalten oder einen Flug genutzt hat, ohne dass Identität für personenscharfe Suche hinreichend geklärt ist). Auch dies könnte in der Gesetzesbegründung verdeutlicht werden, ohne dass es spezieller Regelung bedarf (da keine speziellen Voraussetzungen gelten sollen).

[9] Reine Bundesregelung, kein Muster für Landesgesetz.

[10] Entspricht § 8b Abs. 8 BVerfSchG.

[11] Nähere Regelungen, wie derzeit in § 2 G 10 enthalten, sollten vorzugsweise - flexibler - in einer VO getroffen werden; bleibt im Hinblick auf Ermächtigungsbestimmtheit zu überprüfen.

[12] Die bisherige Regelung des Spezialitätsverhältnisses in § 8b VIII S. 4 f. erscheint überdetailliert; bleibt zu prüfen.

a) die Voraussetzungen für die Anwendung des Verfahrens,

b) das Nähere über Form, Inhalt, Verarbeitung und Sicherung der zu übermittelnden Daten,

c) die Art und Weise der Übermittlung der Daten,

d) die Zuständigkeit für die Entgegennahme der zu übermittelnden Daten,

e) der Umfang und die Form der für dieses Verfahren erforderlichen besonderen Erklärungspflichten des Auskunftspflichtigen und

f) Tatbestände und Bemessung einer auf Grund der Auskunftserteilung an Verpflichtete zu leistenden Aufwandsentschädigung.

Zur Regelung der Datenübermittlung kann in der Rechtsverordnung auf Veröffentlichungen sachverständiger Stellen verwiesen werden; hierbei sind das Datum der Veröffentlichung, die Bezugsquelle und eine Stelle zu bezeichnen, bei der die Veröffentlichung archivmäßig gesichert niedergelegt ist.]

(5) [Eventuell Regelung entsprechend § 8b IX BVerfSchG; bleibt rechtspolitisch zu überprüfen.[13]]

[13] Unterschiedliche Regelungen in den Ländern. Im Vergleich mit anderen Bürokratielasten, die der Staat auch nicht durch Entgelt kompensiert, erscheinen Entschädigungen in den vorliegenden Sachverhalten, soweit nicht bereits über § 110 TKG abzugelten, eher überzogen.

8	Alternative Regelungsvorschläge

§ Y Nachrichtendienstliche Mittel (als Alternative zu § X)

(**1**) [1]Die Verfassungsschutzbehörde darf zur Erhebung personenbezogener Daten nur[1] folgende nachrichtendienstliche Mittel einsetzen[2]:

1. verdeckte Ermittlungen bei Betroffenen und Dritten unter den Voraussetzungen des § Y+1;

2. verdecktes Mithören ohne Inanspruchnahme technischer Mittel unter den Voraussetzungen des § Y+1;

3. Teilnahme an einer Kommunikationsbeziehung im Internet unter einer Legende (Absatz 2 Satz 1 Nr. 1) und unter Ausnutzung eines schutzwürdigen Vertrauens der oder des Betroffenen oder Dritten, um ansonsten nicht zugängliche Daten zu erhalten, unter den Voraussetzungen des § Y+1;

4. planmäßig angelegte verdeckte Personenbeobachtung (Observation), auch unter Einsatz besonderer für Observationszwecke bestimmter technischer Mittel, soweit dieser Einsatz allein der Bestimmung des jeweiligen Aufenthaltsortes der beobachteten Person dient, unter den Voraussetzungen des § Y+1;

5. einzelne verdeckt angefertigte fotografische Bildaufzeichnungen außerhalb von Wohnungen unter den Voraussetzungen des § Y+1;

6. Inanspruchnahme von

a) Personen, deren planmäßig angelegte Zusammenarbeit mit der Verfassungsschutzbehörde Dritten nicht bekannt ist (Vertrauensleute),

b) Personen, die in Einzelfällen Hinweise geben und deren Zusammenarbeit mit der Verfassungsschutzbehörde Dritten nicht bekannt ist (sonstige geheime Informantinnen und Informanten),

c) Personen mit einer bereits bestehenden Verbindung zu einem Nachrichtendienst einer fremden Macht, die zum Zweck der Spionageabwehr überworben worden sind (überworbene Agentinnen und Agenten), sowie

[1] Es wird vorgeschlagen, die nd-Mittel abschließend im Gesetz zu regeln. Dies bietet ein hohes Maß an Transparenz für die Bürgerin und den Bürger, ohne die Wirksamkeit der Maßnahmen zu beeinträchtigen.
[2] Der besseren Übersichtlichkeit bietet es sich an, die nd-Mittel entsprechend der Eingriffstiefe zu ordnen.

d) Personen, die der Verfassungsschutzbehörde logistische oder sonstige Hilfe leisten, ohne Vertrauenspersonen, sonstige geheime Informantinnen oder Informanten oder überworbene Agentinnen oder Agenten zu sein (Gewährspersonen),

unter den Voraussetzungen der §§ Y+1 und Y+2;

7. Observation, die innerhalb einer Woche insgesamt länger als 24 Stunden oder über einen Zeitraum von einer Woche hinaus durchgeführt wird (längerfristige Observation) oder bei der besondere für Observationszwecke bestimmte technische Mittel zu einem anderen als dem in Nummer 4 genannten Zweck eingesetzt werden, unter den Voraussetzungen der §§ Y+1 und Y+3;

8. verdeckt angefertigte Bildübertragungen und Bildaufzeichnungen außerhalb von Wohnungen, die nicht unter Nummer 5 fallen, unter den Voraussetzungen der §§ Y+1 und Y+3;

9. Einsatz von hauptamtlichen Beschäftigten der Verfassungsschutzbehörde, die planmäßig angelegt und langfristig unter einer Legende (Absatz 2 Satz 1 Nr. 1) personenbezogene Daten erheben (verdeckte Ermittlerinnen und Ermittler), unter den Voraussetzungen der §§ Y+1 und Y+4;

10. verdecktes Mithören und Aufzeichnen des nicht öffentlich gesprochenen Wortes unter Einsatz technischer Mittel außerhalb von Wohnungen unter den Voraussetzungen der §§ Y+1 und Y+5;

11. technische Mittel, mit denen zur Ermittlung der Geräte- und der Kartennummern aktiv geschaltete Mobilfunkendeinrichtungen zur Datenabsendung an eine Stelle außerhalb des Telekommunikationsnetzes veranlasst werden, unter den Voraussetzungen der §§ Y+1 und Y+5;

12. Beobachtung des Funkverkehrs auf nicht für den allgemeinen Empfang bestimmten Kanälen unter den Voraussetzungen der §§ Y+1 und Y+5;

13. Überwachung des Brief-, Post- und Fernmeldeverkehrs unter den Voraussetzungen der §§ Y+1 und X+3,

14. heimliche Erhebung von Daten aus einem informationstechnischen System unter den Voraussetzungen der §§ Y+1 und X+4

15. heimliche Erhebung von Daten aus Wohnungen unter den Voraussetzungen der §§ Y+1 und X+5

[2]Die durch den Einsatz besonderer für Observationszwecke bestimmter technischer Mittel nach Satz 1 Nr. 4 erhobenen Daten dürfen nicht zu einem Bewegungsbild

verbunden werden[3]. [3]Die in Satz 1 Nrn. 5 und 8 genannten Mittel dürfen nicht gegen Versammlungen eingesetzt werden.

(**2**) [1]Soweit es für den Einsatz eines nachrichtendienstlichen Mittels nach Absatz 1 erforderlich ist, darf die Verfassungsschutzbehörde[4]

1. fingierte biografische, berufliche oder gewerbliche Angaben (Legende) mit Ausnahme solcher beruflichen Angaben verwenden, die sich auf Berufsgeheimnisträgerinnen oder Berufsgeheimnisträger nach § 53 StPO oder Berufshelferinnen oder Berufshelfer nach § 53a StPO beziehen, und

2. Tarnpapiere und Tarnkennzeichen beschaffen, herstellen und verwenden.

[2]Tarnpapiere und Tarnkennzeichen dürfen auch zum Schutz der Beschäftigten, Einrichtungen und Gegenstände der Verfassungsschutzbehörde sowie zum Schutz der in Absatz 1 Satz 1 Nr. 6 genannten Personen beschafft, hergestellt und verwendet werden. *{[3]Die Behörden des Landes und der Kommunen sind verpflichtet, der Verfassungsschutzbehörde technische Hilfe bei der Beschaffung und Herstellung von Tarnpapieren und Tarnkennzeichen zu leisten[5].}*

§ Y+1 Allgemeine Voraussetzungen für den Einsatz nachrichtendienstlicher Mittel (als Teilalternative zu § X+1)[6]

(**1**) [1]Der Einsatz eines nachrichtendienstlichen Mittels ist unzulässig, wenn die Erforschung des Sachverhalts auf andere, die Betroffenen weniger beeinträchtigende Weise möglich ist; dies ist in der Regel anzunehmen, wenn die Information aus allgemein zugänglichen Quellen erhoben oder durch ein Ersuchen beschafft werden kann. [2]Der Einsatz eines nachrichtendienstlichen Mittels darf nicht erkennbar außer Verhältnis zur Bedeutung des aufzuklärenden Sachverhalts stehen, insbesondere nicht außer Verhältnis zu der Gefahr, die von der Bestrebung[7] oder der Tätigkeit nach § 3 Abs. 1 Nr. 2 ausgeht oder ausgehen kann. [3]Der Einsatz eines nachrichtendienstlichen Mittels ist unverzüglich zu beenden, wenn sein Zweck erreicht ist oder sich Anhaltspunkte dafür ergeben, dass er nicht oder nicht auf diese Weise erreicht werden kann.

---

[3] § Y Abs. 1 Satz 2 dient der Abgrenzung der Ziffer 4 von der Ziffer 7

[4] Tarnmittel sind Hilfsmittel zur Arbeit des VS, daher gesondert von den nd-Mitteln zu regeln.

[5] Eine spezifische Regelung für Flächenländer.

[6] Zudem müssten allgemeine Regelungen zur Datenerhebung außerhalb der nd-Mittel sowie der Kernbereichs- und Minderjährigenschutz gesondert geregelt werden (§§ Y+1a, Y+1b und Y+1c)

[7] Alternativ bietet sich an, im Gesetz das Beobachtungsobjekt als Bezugspunkt der Aufklärungsarbeit zu definieren und formal zu bestimmen, sodass dann die Eingriffsschwellen direkt in Bezug gesetzt werden können. Dabei könnten zudem als Vorphase das Verdachtsobjekt und eine Verdachtsgewinnungsphase mit jeweils eingeschränkten Befugnissen angelegt werden (vergl. §§ 6ff. NVerfSchG).

(**2**) [1]Ein nachrichtendienstliches Mittel darf nur eingesetzt werden, wenn

1. sich der Einsatz gegen Personenzusammenschlüsse, in ihnen oder für sie tätige Personen oder gegen Einzelpersonen richtet, bei denen tatsächliche Anhaltspunkte für den Verdacht von Bestrebungen oder Tätigkeiten nach § 3 Abs. 1 bestehen oder,

2. sich der Einsatz gegen eine Person richtet, von der aufgrund bestimmter Tatsachen anzunehmen ist, dass sie mit einer der in Nummer 1 genannten Personen in Verbindung steht und dass deshalb der Einsatz des Mittels unumgänglich[8] ist, um Erkenntnisse über eine Bestrebung von erheblicher Bedeutung oder über eine Tätigkeit nach § 3 Abs. 1 Nr. 2 zu gewinnen,

3. dadurch die zur planmäßigen Beobachtung und Aufklärung einer Bestrebung oder zur Erfüllung der Aufgabe nach § 3 Abs. 1 Nr. 2 erforderlichen Vertrauenspersonen, sonstigen geheimen Informantinnen und Informanten, überworbenen Agentinnen und Agenten sowie Gewährspersonen gewonnen oder überprüft werden können oder

5. dies zum Schutz der Beschäftigten, Einrichtungen und Gegenstände der Verfassungsschutzbehörde sowie zum Schutz der Vertrauenspersonen, sonstigen geheimen Informantinnen und Informanten, überworbenen Agentinnen und Agenten sowie Gewährspersonen erforderlich ist.

[2]Ein nachrichtendienstliches Mittel darf auch eingesetzt werden, wenn Dritte unvermeidbar betroffen werden.

(**3**) Bei dem Einsatz eines nachrichtendienstlichen Mittels dürfen die Beschäftigten der Verfassungsschutzbehörde keine Straftaten begehen.

(**4**) Die Zielsetzung und die Aktivitäten von Bestrebungen dürfen von der Verfassungsschutzbehörde weder unmittelbar noch mittelbar steuernd beeinflusst werden.

---

[8] Da es verfassungsrechtlich problematisch ist, wenn sich schwerwiegende Grundrechtseingriffe durch gezielten Einsatz nachrichtendienstlicher Mittel gegen Kontakt- und Begleitpersonen nach den nahezu gleichen Voraussetzungen richten wie gegen die Verdachtspersonen selbst, muss ein weiteres Kriterium hinzukommen. Die gesetzliche Ausgestaltung muss sich daran orientieren, dass die Kontaktpersonen nur insoweit von Interesse sind, als sie Aufschluss über die Hauptperson vermitteln können (vgl. dazu BVerfGE 133, 277, 349 f.; auch schon BVerfGE 113, 348, 380 f.; zur Problematik näher Bergemann, in Handbuch des Polizeirechts, 5. Aufl., H Rn. 53 ff. m. w. N., zur Abstufung z. B. § 34 Abs. 1 Satz 1 Nrn. 2 und 3 Nds. SOG). Das einfache Abstellen auf den Empfang und die Weitergabe von Mitteilungen ist für eine solche Begrenzung ungeeignet, da diese Vorgabe in erster Linie auf die - im Artikel 10-Gesetz geregelte - Post- und Telekommunikationsüberwachung zugeschnitten ist (vgl. § 3 Abs. 2 Satz 2 G 10), jedoch zur Rechtfertigung des Einsatzes sonstiger nachrichtendienstlichen Mittel nur bedingt passen dürfte (Alternativformulierung zu „unumgänglich“ vgl. beispielhaft die Regelung des § 163 f Abs. 1 Satz 3 StPO zur längerfristigen Observation).

§ Y+1a Allgemeine Befugnis zur Datenerhebung (als Teilalternative zu § X+1)

(**1**) Die Verfassungsschutzbehörde darf die zu einer planmäßigen Beobachtung und Aufklärung einer Bestrebung oder Tätigkeit {*eines Prüffalles/Einzelpersonen*} erforderlichen personenbezogenen Daten erheben, soweit in den Vorschriften dieses Kapitels nicht anderes geregelt ist.

(**2**) [1]Werden personenbezogene Daten bei Betroffenen mit deren Kenntnis erhoben, so ist der Erhebungszweck anzugeben. [2]Werden personenbezogene Daten bei Dritten außerhalb des öffentlichen Bereichs erhoben, so ist der Erhebungszweck auf deren Verlangen anzugeben. [3]Die Betroffenen und die Dritten sind auf die Freiwilligkeit ihrer Angaben hinzuweisen.

(**3**) Ist zum Zweck der Erhebung die Übermittlung personenbezogener Daten unerlässlich, so dürfen schutzwürdige Interessen der Betroffenen nur im unvermeidbaren Umfang beeinträchtigt werden.

§ Y+1b Schutz des Kernbereichs privater Lebensgestaltung (als Teilalternative zu § X+1)

(**1**) Eine Datenerhebung darf nicht angeordnet werden, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass dadurch {*nicht nur zufällig/nicht allein*} Daten erhoben werden, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind.

(**2**) [1]Wenn sich während einer bereits laufenden Datenerhebung tatsächliche Anhaltspunkte dafür ergeben, dass Daten aus dem Kernbereich privater Lebensgestaltung erhoben werden, ist die Datenerhebung unverzüglich und so lange wie erforderlich zu unterbrechen, soweit dies informationstechnisch möglich ist und dadurch die Datenerhebung den Betroffenen nicht bekannt wird. [2]Bereits erhobene Daten aus dem Kernbereich privater Lebensgestaltung dürfen nicht gespeichert, verändert, genutzt oder übermittelt werden; sie sind unverzüglich unter Aufsicht einer oder eines besonders bestellten, mit der Auswertung nicht befassten Beschäftigten, die oder der die Befähigung zum Richteramt hat, zu löschen. [3]Die Tatsache, dass Daten aus dem Kernbereich privater Lebensgestaltung erhoben wurden, und deren Löschung sind zu dokumentieren. [4]Die in der Dokumentation enthaltenen Daten dürfen ausschließlich zur Datenschutzkontrolle verwendet werden. [5]Sie sind zu löschen, wenn seit einer Mitteilung nach § X+10 ein Jahr vergangen ist oder es einer Mitteilung gemäß § X+10 Abs. 3 endgültig nicht bedarf, frühestens jedoch zwei Jahre nach der Dokumentation.

(**3**) Ergeben sich erst bei der Speicherung, Veränderung oder Nutzung von Daten tatsächliche Anhaltspunkte dafür, dass Daten dem Kernbereich privater Lebensgestaltung zuzurechnen sind, so gilt Absatz 2 Sätze 2 bis 5 entsprechend.

(**4**) Daten aus dem durch das Berufsgeheimnis geschützten Vertrauensverhältnis nach den §§ 53 und 53a der Strafprozessordnung (StPO) sind dem Kernbereich privater Lebensgestaltung zuzurechnen.

(**5**) Bestehen Zweifel, ob Daten dem Kernbereich privater Lebensgestaltung zuzurechnen sind, so sind diese der Leiterin oder dem Leiter der Verfassungsschutzabteilung zur Entscheidung über die Zurechnung vorzulegen.

§ Y+1c Erhebung personenbezogener Daten von Minderjährigen (als Teilalternative zu § X+1)[9]

(**1**) Die Erhebung von personenbezogenen Daten über eine minderjährige Person, die das 14. Lebensjahr noch nicht vollendet hat, ist unzulässig.

(**2**) Die Erhebung von Daten über eine minderjährige Person, die das 14. Lebensjahr, aber noch nicht das 16. Lebensjahr vollendet hat, ist nur zulässig, wenn

1. tatsächliche Anhaltspunkte für den Verdacht bestehen, dass sie eine Straftat nach § 3 Abs. 1 des Artikel 10-Gesetzes plant, begeht oder begangen hat,

2. nach den Umständen des Einzelfalls nicht ausgeschlossen werden kann, dass die Erhebung zur Abwehr einer Gefahr für Leib oder Leben erforderlich ist, oder

3. tatsächliche Anhaltspunkte dafür bestehen, dass sie eine Tätigkeit nach § 3 Abs. 1 Nr. 2 ausübt.

(**3**) Die Erhebung von Daten über eine minderjährige Person, die das 16. Lebensjahr vollendet hat, ist nur zulässig, wenn tatsächliche Anhaltspunkte dafür bestehen, dass sie

1. in einem oder für ein Beobachtungs- oder Verdachtsobjekt tätig ist, das auf die Anwendung oder Vorbereitung von Gewalt gerichtet ist, und sie diese Ausrichtung fördert,

2. in herausgehobener Funktion in einem Beobachtungs- oder Verdachtsobjekt tätig ist oder

3. eine Tätigkeit nach § 3 Abs. 1 Nr. 2 ausübt.

(**4**) [1]Die Datenerhebung darf kein Verhalten einer Person aus der Zeit vor Vollendung ihres 14. Lebensjahres erfassen. [2]Das Verhalten einer Person aus der Zeit zwischen

[9] Der an der NI-Regelung orientierte Alternativvorschlag differenziert zwischen drei Altersklassen. Dabei reduziert sich die Erhebungsschwelle mit steigendem Alter, orientiert an der altersgemäßen Entwicklung der Minderjährigen. Vor Vollendung des 14. Lebensjahres ist die Datenerhebung ausnahmslos unzulässig (vergl. §Y+1c Abs. 4). Korrespondierend mit dem gesetzlichen Auftrag des VS in Abgrenzung zur polizeilichen Gefahrenabwehr entsteht dadurch keine Sicherheitslücke, da konkrete Gefahren unabhängig davon durch die Polizei abgewehrt werden können. Vergl. hierzu im Übrigen im Bericht :"*4.1.Votum für eine Beibehaltung der derzeitigen Rechtslage*".

Vollendung ihres 14. und 16. Lebensjahres darf die Datenerhebung nur erfassen, wenn zum Zeitpunkt dieses Verhaltens die Voraussetzungen des Absatzes 2 vorlagen. [3]Das Verhalten einer Person aus der Zeit zwischen Vollendung ihres 16. und 18. Lebensjahres darf die Datenerhebung nur erfassen, wenn zum Zeitpunkt dieses Verhaltens die Voraussetzungen des Absatzes 3 vorlagen.

(**5**) Die Absätze 1 bis 4 gelten nicht, soweit minderjährige Personen von der Datenerhebung unvermeidbar als Dritte betroffen werden.

§ Y+3 Besondere Voraussetzungen für Observationen sowie Bildübertragungen und Bildaufzeichnungen (als Teilalternative und Ergänzung zu § X und § X+9)

Die Verfassungsschutzbehörde darf die nachrichtendienstlichen Mittel der Observation nach § Y Abs. 1 Satz 1 Nr. 7 sowie der Bildübertragungen und Bildaufzeichnungen nach § Y Abs. 1 Satz 1 Nr. 8 nur einsetzen, um Erkenntnisse über eine Bestrebung, welche auf die Anwendung oder Vorbereitung von Gewalt gerichtet ist oder aus anderen Gründen erhebliche Bedeutung hat, oder über eine Tätigkeit nach § 3 Abs. 1 Nr. 2 zu gewinnen.

§ Y+4 Besondere Voraussetzungen für den Einsatz verdeckter Ermittlerinnen und Ermittler (als Teilalternative und Ergänzung zu § X und § X+9)[10]

(**1**) Eine verdeckte Ermittlerin oder ein verdeckter Ermittler darf nur unter den Voraussetzungen des § 1 Abs. 1 Nr. 1 und des § 3 Abs. 1 des Artikel 10-Gesetzes eingesetzt werden.

(**2**) [1]Der Einsatz einer verdeckten Ermittlerin oder eines verdeckten Ermittlers ist fortlaufend zu dokumentieren. [2]§ Y+2 Abs. 4 gilt für verdeckte Ermittlerinnen und Ermittler entsprechend.

§ Y+5 Besondere Voraussetzungen für den Einsatz bestimmter technischer Mittel (als Teilalternative und Ergänzung zu § X und § X+9)

(**1**) Die Verfassungsschutzbehörde darf ein technisches Mittel nach § Y Abs. 1 Satz 1 Nrn. 10 bis 12 nur unter den Voraussetzungen des § 1 Abs. 1 Nr. 1 und des § 3 Abs. 1 des Artikel 10-Gesetzes einsetzen.

[10] Verdeckte Ermittler sind aufgrund des gegenüber Vertrauensleuten höheren Grundrechtseingriffs von den Vertrauensleuten gesondert zu regeln.

(**2**) Der Einsatz eines technischen Mittels nach § Y Abs. 1 Satz 1 Nr. 11 darf sich nur gegen eine Person richten, bei der

1. tatsächliche Anhaltspunkte für den Verdacht bestehen, dass sie eine Straftat nach § 3 Abs. 1 des Artikel 10-Gesetzes plant, begeht oder begangen hat, oder

2. aufgrund bestimmter Tatsachen anzunehmen ist, dass sie über ihren Teilnehmeranschluss für eine Person nach Nummer 1 bestimmte oder von ihr herrührende Mitteilungen entgegennimmt oder weitergibt oder dass eine Person nach Nummer 1 ihren Teilnehmeranschluss nutzt, und dass deshalb der Einsatz unumgänglich[11] ist, um Erkenntnisse über ein Beobachtungs- oder Verdachtsobjekt oder über eine Tätigkeit nach § 3 Abs. 1 Nr. 2 zu gewinnen.

§ Y+6 Besondere Auskunftsersuchen[12] (als Alternative zu § X+11)

(**1**) [1]Die Verfassungsschutzbehörde kann anordnen, dass ein Diensteanbieter nach § 2 Satz 1 Nr. 1 des Telemediengesetzes (TMG) ihr Auskunft erteilt

1. zu Bestandsdaten (§ 14 TMG) oder
2. zu Nutzungsdaten (§ 15 Abs. 1 TMG).

[2]Die Erteilung einer Auskunft nach Satz 1 darf nur im Einzelfall und unter der Voraussetzung angeordnet werden, dass sie zu einer planmäßigen Beobachtung und Aufklärung einer Bestrebung oder zur Erfüllung der Aufgabe nach § 3 Abs. 1 Nr. 2 erforderlich ist und dass tatsächliche Anhaltspunkte für eine schwerwiegende Gefahr für ein in § 3 Abs. 1 genanntes Schutzgut vorliegen. [3]Zur Erfüllung der Aufgabe nach § 3 Abs. 1 Nr. 1 darf die Erteilung einer Auskunft zu Nutzungsdaten nur angeordnet werden, wenn die Bestrebung auf die Anwendung oder Vorbereitung von Gewalt gerichtet ist oder aus anderen Gründen erhebliche Bedeutung hat. [4]Die Erteilung einer Auskunft zu Nutzungsdaten darf nur zu einer Person angeordnet werden,

1. bei der tatsächliche Anhaltspunkte dafür vorliegen, dass sie die schwerwiegende Gefahr nachdrücklich fördert, oder
2. bei der aufgrund bestimmter Tatsachen anzunehmen ist, dass sie Telemedien für eine Person nach Nummer 1 nutzt und dass deshalb die Anordnung unumgänglich[13] ist, um Erkenntnisse über eine Bestrebung oder über eine Tätigkeit zu gewinnen.

---

[11] Siehe Anmerkung zu § Y+1 Abs. 2

[12] Mitwirkungspflichten und Auskunftsersuchen sind Teil der Datenerhebung der Verfassungsschutzbehörde. Sie gehören systematisch zu den nachrichtendienstlichen Mitteln. Dies erleichtert das Auffinden der jeweiligen Rechtsgrundlagen erheblich. Zudem sollte an den Wortlaut der jeweiligen Öffnungsvorschriften der Fachgesetze angeknüpft werden. Dies zusammen eröffnet zudem die Möglichkeit eines wesentlich differenzierteren Systems von Eingriffsvoraussetzungen, mittels dessen der jeweiligen Eingriffsintensität wesentlich besser Rechnung getragen werden kann.

[13] Siehe Anmerkung zu § Y+1 Abs. 2

(**2**) [1]Die Verfassungsschutzbehörde kann anordnen, dass ein Diensteanbieter nach § 3 Nr. 6 des Telekommunikationsgesetzes (TKG) ihr Auskunft erteilt

1. zu den nach den §§ 95 und 111 TKG erhobenen Bestandsdaten (einfache Bestandsdaten),
2. zu Bestandsdaten nach Nummer 1, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird oder die anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse bestimmt werden (besondere Bestandsdaten), oder
3. zu Verkehrsdaten nach § 96 Abs. 1 Nrn. 1 bis 4 TKG und sonstigen zum Aufbau und zur Aufrechterhaltung der Telekommunikation notwendigen Verkehrsdaten.

[2]Die Erteilung einer Auskunft nach Satz 1 darf nur angeordnet werden, wenn sie im Einzelfall zu einer planmäßigen Beobachtung und Aufklärung einer Bestrebung oder zur Erfüllung der Aufgabe nach § 3 Abs. 1 Nr. 2 erforderlich ist. [3]Die Erteilung einer Auskunft zu besonderen Bestandsdaten und zu Verkehrsdaten darf nur unter den Voraussetzungen des § 1 Abs. 1 Nr. 1 und des § 3 Abs. 1 des Artikel 10-Gesetzes und nur zu einer Person angeordnet werden, bei der

1. tatsächliche Anhaltspunkte für den Verdacht bestehen, dass sie eine Straftat nach § 3 Abs. 1 des Artikel 10-Gesetzes plant, begeht oder begangen hat,
2. aufgrund bestimmter Tatsachen anzunehmen ist, dass sie über ihren Teilnehmeranschluss für eine Person nach Nummer 1 bestimmte oder von ihr herrührende Mitteilungen entgegennimmt oder weitergibt oder dass eine Person nach Nummer 1 ihren Teilnehmeranschluss nutzt und dass deshalb die Anordnung unumgänglich[14] ist, um Erkenntnisse über ein Beobachtungs- oder Verdachtsobjekt oder über eine Tätigkeit nach § 3 Abs. 1 Nr. 2 zu gewinnen.

(**3**) [1]Die Verfassungsschutzbehörde kann anordnen, dass

1. Luftfahrtunternehmen
2. Unternehmen der Finanzbranche Auskunft zu Konten und Geldanlagen, insbesondere zu Kontoständen, Zahlungsein- und -ausgängen und sonstigen Geldbewegungen, sowie zu Kontoinhaberinnen, Kontoinhabern, sonstigen Berechtigten und weiteren am Zahlungsverkehr Beteiligten, erteilen. [2]Zur Auskunft nach Nummer 1 sind ebenso die Betreiber von Computerreservierungssystemen und Globalen Distributionssystemen verpflichtet. [3]Die Erteilung einer Auskunft nach Satz 1 darf nur im Einzelfall und unter der Voraussetzung angeordnet werden, dass sie zu einer planmäßigen Beobachtung und Aufklärung einer Bestrebung oder zur Erfüllung der Aufgabe nach § 3 Abs. 1 Nr. 2 erforderlich ist und dass tatsächliche Anhaltspunkte für eine schwerwiegende Gefahr für ein in § 3 Abs. 1 genanntes

[14] Siehe Anmerkung zu § Y+1 Abs. 2

Schutzgut vorliegen; Absatz 1 Satz 3 gilt entsprechend. [4]Die Erteilung einer Auskunft nach Satz 1 darf nur zu einer Person angeordnet werden, bei der

1. tatsächliche Anhaltspunkte dafür vorliegen, dass sie die schwerwiegende Gefahr nachdrücklich fördert, oder
2. aufgrund bestimmter Tatsachen anzunehmen ist, dass sie eine in Satz 1 genannte Dienstleistung für eine Person nach Nummer 1 in Anspruch nimmt und dass deshalb die Anordnung unumgänglich[15] ist, um Erkenntnisse über ein Beobachtungs- oder Verdachtsobjekt oder über eine Tätigkeit nach § 3 Abs. 1 Nr. 2 zu gewinnen.

(**4**) [1]Auskünfte nach den Absätzen 1 und 3 sind unentgeltlich zu erteilen. [2] Die Verfassungsschutzbehörde hat für die Erteilung von Auskünften nach Absatz 2 eine Entschädigung entsprechend § 23 des Justizvergütungs- und -entschädigungsgesetzes zu gewähren.

(**5**) Anordnungen nach den Absätzen 1 bis 3 und die übermittelten Daten dürfen den Betroffenen oder Dritten von den Verpflichteten nicht mitgeteilt werden.

(**6**) [1]Den Verpflichteten ist es verboten, allein aufgrund einer Anordnung nach den Absätzen 1 bis 3 einseitige Handlungen vorzunehmen, die für die Betroffene oder den Betroffenen nachteilig sind und die über die Erteilung der Auskunft hinausgehen, insbesondere bestehende Verträge oder Geschäftsverbindungen zu beenden, ihren Umfang zu beschränken oder ein Entgelt zu erheben oder zu erhöhen. [2]Die Anordnung ist mit dem ausdrücklichen Hinweis auf dieses Verbot und darauf zu verbinden, dass das Auskunftsersuchen nicht die Aussage beinhaltet, dass sich die betroffene Person rechtswidrig verhalten hat oder ein darauf gerichteter Verdacht besteht.

[15] Siehe Anmerkung zu § Y+1 Abs. 2